

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平7-191940

(43)公開日 平成7年(1995)7月28日

(51)Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 15/00	3 3 0 G	7459-5L		
	D	7459-5L		

審査請求 未請求 請求項の数15 O L (全 17 頁)

(21)出願番号 特願平5-332655

(22)出願日 平成5年(1993)12月27日

(71)出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72)発明者 廣瀬 浩一

鎌倉市上町屋325番地 三菱電機株式会社

コンピュータ製作所内

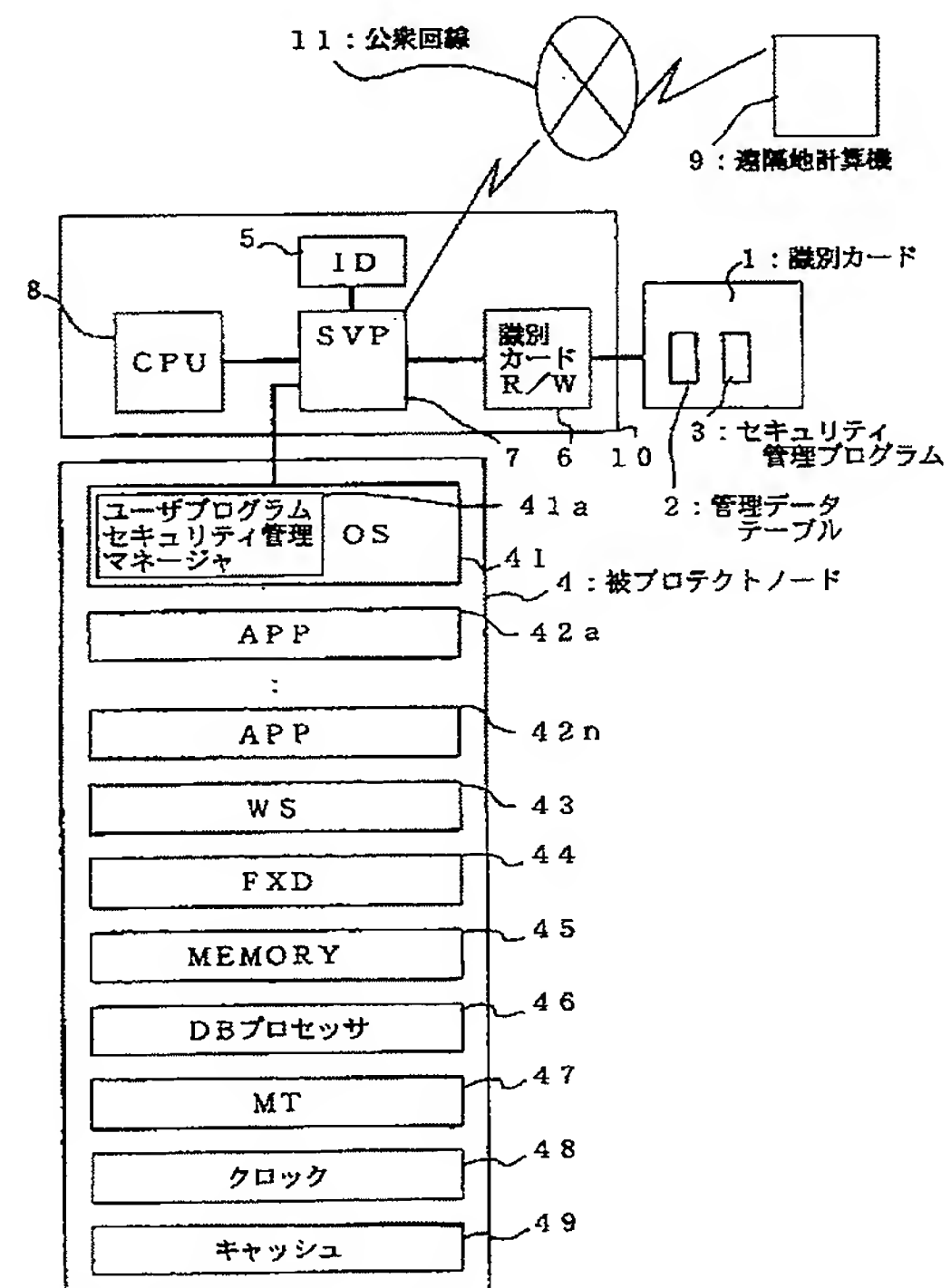
(74)代理人 弁理士 高田 守

(54)【発明の名称】 計算機の資源利用方式

(57)【要約】

【目的】 オプションH/W或は計算機S/Wの不法な使用を防止し、識別カードを使用することにより、管理データテーブルの不法改竄の抑止効果を向上させる。

【構成】 識別カード1の管理データテーブル2には、被プロテクトノード4（オプションのH/W、及びS/W）の使用可否、及び使用期限等のデータが入っている。システム立ち上げ時にセキュリティー管理プログラム3とSVP7は計算機筐体に設けられた個別の識別子5と識別カード1に格納された個別の識別子との認証を行ない、指定された識別番号を送ってきた計算機に対してのみ管理データテーブルのアクセスを許可する。整合がとれなければそこで、システム立ち上げを中止する。



【特許請求の範囲】

【請求項 1】 以下の要素を有する計算機の資源利用方式

(a) 計算機を個別に識別する識別子を計算機に格納する識別子格納手段、(b) 上記識別子と同一の識別子と、計算機が利用できる資源を被プロテクトノードとして定義した管理データテーブルを保持する識別カード、(c) 上記識別カードに保持された識別子を計算機に入力して上記識別子格納手段により格納された識別子と比較して、一致した場合に、計算機から上記識別カードに保持された管理データテーブルをアクセスし、計算機に対して管理データテーブルに定義された資源の利用を認める利用許可手段。

【請求項 2】 上記利用許可手段は、計算機の起動時に、上記識別子格納手段により格納された識別子と上記識別カードに保持された識別子と比較して、管理データテーブルの内容を読みだし、読み出した管理データテーブルの内容を参照して計算機のシステム構成を決定するサービスプロセッサを備えたことを特徴とする請求項 1 記載の計算機の資源利用方式。

【請求項 3】 上記サービスプロセッサは、識別カードから読み込んだ管理データテーブルの内容を記憶するとともに、記憶した管理データテーブルの内容を参照して使用するオペレーティングシステムをインストールするとともに、上記被プロテクトノードの起動要求に対して、被プロテクトノードの起動の可否を決定することを特徴とする請求項 2 記載の計算機の資源利用方式。

【請求項 4】 上記識別カードは、アプリケーションプログラムを上記被プロテクトノードとして定義し、上記オペレーティングシステムは、アプリケーションプログラムの起動要求に対する管理データテーブルの参照をサービスプロセッサとの通信により行うセキュリティ管理マネージャを備え、セキュリティ管理マネージャが管理データテーブルを参照してアプリケーションプログラムの起動の許可を与えることを特徴とする請求項 3 記載の計算機の資源利用方式。

【請求項 5】 上記識別カードは、接続端末を上記被プロテクトノードとして定義し、上記利用許可手段は、接続端末の接続制限をサービスプロセッサに行わせることを特徴とする請求項 2 記載の計算機の資源利用方式。

【請求項 6】 上記識別カードは、ディスク記憶装置を上記被プロテクトノードとして定義し、上記利用許可手段は、ディスク記憶装置の接続制限をサービスプロセッサに行わせることを特徴とする請求項 2 記載の計算機の資源利用方式。

【請求項 7】 上記識別カードは、主記憶装置容量を上記被プロテクトノードとして定義し、上記利用許可手段は、主記憶装置容量の接続制限をサービスプロセッサに行わせることを特徴とする請求項 2 記載の計算機の資源利用方式。

【請求項 8】 上記識別カードは、接続データベースプロセッサを上記被プロテクトノードとして定義し、上記利用許可手段は、接続データベースプロセッサの接続制限をサービスプロセッサに行わせることを特徴とする請求項 2 記載の計算機の資源利用方式。

【請求項 9】 上記識別カードは、テープ装置を上記被プロテクトノードとして定義し、上記利用許可手段は、テープ装置の接続制限をサービスプロセッサに行わせることを特徴とする請求項 2 記載の計算機の資源利用方式。

【請求項 10】 上記識別カードは、計算機クロック周波数を上記被プロテクトノードとして定義し、上記利用許可手段は、計算機クロック周波数の設定をサービスプロセッサに行わせることを特徴とする請求項 2 記載の計算機の資源利用方式。

【請求項 11】 上記識別カードは、キャッシュメモリを上記被プロテクトノードとして定義し、上記利用許可手段は、キャッシュメモリの設定をサービスプロセッサに行わせることを特徴とする請求項 2 記載の計算機の資源利用方式。

【請求項 12】 上記識別子格納手段は、識別子を書き換え可能な不揮発性メモリに格納しサービスプロセッサの固有な手続きにより識別子を書換え可能としたことを特徴とする請求項 1 記載の計算機の資源利用方式。

【請求項 13】 上記計算機の資源利用方式は、少なくとも上記識別カードの識別子および管理データテーブルの内容のどちらか一方を計算機から更新できることを特徴とする請求項 1 記載の計算機の資源利用方式。

【請求項 14】 上記識別カードを、利用許可手段と独自に通信できる通信手段を有する専用不揮発性記憶媒体カードとしたことを特徴とする請求項 1 記載の計算機の資源利用方式。

【請求項 15】 識別カードと利用許可手段間を独自のインタフェースにより接続したことを特徴とする請求項 1 記載の計算機の資源利用方式。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、計算機において、ソフトウェアやハードウェア等の資源を利用するための計算機の資源利用システムに関するものである。特にロードするソフトウェア（以下、S/W）、あるいは接続するハードウェア（以下、H/W）に制限を与えるプログラムロード方式及びH/Wインストール方式に関するものである。

【0002】

【従来の技術】 セキュリティ機能を有する計算機システムについては、技術文献にしばしば見られる。例えば、特開平 3 - 2 3 7 5 5 1 には、トランザクションシステムセキュリティ方法及び装置に関する内容が記述されている。上記技術は、システムコンポーネントの確認、ユ

3

ーザ識別の証明、ユーザ許可及びアクセス制御を識別カードを使用して実現しようとするものである。

【0003】また、たとえば、特開平4-255030には、プログラムロード方式に関する内容が記述されている。上記技術は、制御プログラムを起動し識別コード入力装置から識別コードが入力されると、制御プログラムが、セキュリティ管理プログラムを起動し、そのセキュリティ管理プログラムにより実行可能なプログラムをロードするものである。

【0004】

【発明が解決しようとする課題】上記技術は、主に被セキュリティプログラムとユーザとの認証をテーマとしており、ローカルに固有な計算機H/Wとそれに付随するS/W、周辺機器との認証まではカバーしない。上記技術における被セキュリティプログラム及び識別カードは複数のH/W上で同様に動作する。また、従来のセキュリティ機能を有する計算機システムは、計算機システムが既に持っている資源を、許可のないユーザによって使われてしまうことを防止するためのものである。あるいは、従来のセキュリティ機能とは、エンドユーザが他のユーザによって、許可なく使われてしまうことを防止するためのものである。一方、このようなエンドユーザのセキュリティ機能という観点とは異なる計算機の資源の利用制限を考える必要がでてきた。ソフトウェアの供給者あるいはハードウェアの供給者は、供給するソフトウェアやハードウェアが、契約された計算機のみで動作するような保証を得たいと考えている。すなわち、契約の対象となったソフトウェアや周辺機器等が契約した顧客の計算機のみで動作するようにし、ソフトウェアやハードウェアの不正使用を防止する必要がある。たとえば、販売されたソフトウェアが不正に他の計算機上で利用されたり、第三者が提供した周辺機器が、不正に計算機に増設されたりする場合があります、このような不正使用を防止する必要がある。

【0005】この発明は、以上のような問題点を解決するためになされたもので、従来のエンドユーザのセキュリティ機能とは異なり、ソフトウェア提供者やハードウェア提供者に対して、提供したソフトウェアやハードウェアが不正に使用されることを防止する計算機の資源利用システムを提供することを目的としている。

【0006】特に、本発明は、固有の当該計算機に対し、一対一に対応する識別カードを持ち、それぞれに固有のS/Wのロードの制限、あるいは周辺機器のインストールに制限を与える手段を提供するものである。

【0007】具体的には、以下の目的を有している。

- ・資源（H/WおよびS/W）の利用は、顧客（マシン）毎に資源利用契約をしてもらう。

- ・ICカードを利用した資源不正使用防止システムを構築する。ICカードシステムを導入し、ICカード中に、利用できる資源、及び、その有効期限等の情報を持

4

ち、それに反する利用はできない仕組みを作りこみ、資源の不正使用を防止するシステムを構築する。

- ・ICカード内の情報を、メーカ内に構築された顧客管理システムにも提供する。その情報を活用し、リプレースの促進、コンサルタント業務の徹底をはかる。また、ICカード再発行時などは、顧客管理システム内の情報をもとにICカードを複製する。

【0008】

【課題を解決するための手段】請求項1記載の発明に係る10 計算機の資源利用方式は、以下の要素を有する。

（a）計算機を個別に識別する識別子を格納する識別子格納手段、（b）上記識別子と同一の識別子と、計算機が利用できる資源を被プロテクトノードとして定義した管理データテーブルを保持する識別カード、（c）上記識別子格納手段により格納された識別子と、上記識別カードに保持された識別子を比較して、一致した場合に、上記識別カードに保持された管理データテーブルをアクセスし、管理データテーブルに定義された資源の利用を認める利用許可手段。

20 【0009】請求項2記載の発明に係る計算機の資源利用方式は、請求項1記載の計算機の資源利用方式において、上記利用許可手段が、計算機の起動時に、上記識別子格納手段により格納された識別子と上記識別カードに保持された識別子を比較して、管理データテーブルの内容を読みだし、読み出した管理データテーブルの内容を参照して計算機のシステム構成を決定するサービスプロセッサを備えたことを特徴とするものである。

30 【0010】請求項3記載の発明に係る計算機の資源利用方式は、請求項2記載の計算機の資源利用方式において、上記サービスプロセッサが、管理データテーブルの内容、すなわち、計算機が利用する資源を被プロテクトノードとして記憶し、使用するオペレーティングシステムをインストールするとともに、上記サービスプロセッサは、上記被プロテクトノードの起動要求に対して記憶した管理データテーブルの内容を参照して被プロテクトノードの起動の可否を決定することを特徴とするものである。

40 【0011】請求項4記載の発明に係る計算機の資源利用方式は、請求項3記載の計算機の資源利用方式において、上記被プロテクトノードをアプリケーションプログラムとし、オペレーティングシステムは、アプリケーションプログラムの起動要求に対する管理データテーブルの認証をサービスプロセッサとの通信により行うセキュリティ管理マネージャを備え、セキュリティ管理マネージャが管理データテーブルとの整合性をチェックしアプリケーションプログラムのロードの許可を与えることを特徴とするものである。

50 【0012】請求項5記載の発明に係る計算機の資源利用方式は、請求項2記載の計算機の資源利用方式において、上記被プロテクトノードを接続端末とし、接続端末

5

の接続制限をサービスプロセッサに行わせることを特徴とするものである。

【0013】請求項6記載の発明に係る計算機の資源利用方式は、請求項2記載の計算機の資源利用方式において、上記被プロテクトノードを接続F X Dとし、接続F X Dの接続制限をサービスプロセッサに行わせることを特徴とするものである。

【0014】請求項7記載の発明に係る計算機の資源利用方式は、請求項2記載の計算機の資源利用方式において、上記被プロテクトノードを主記憶装置容量とし、主記憶装置容量の接続制限をサービスプロセッサに行わせることを特徴とするものである。

【0015】請求項8記載の発明に係る計算機の資源利用方式は、請求項2記載の計算機の資源利用方式において、上記被プロテクトノードを接続データベースプロセッサとし、接続データベースプロセッサの接続制限をサービスプロセッサに行わせることを特徴とするものである。

【0016】請求項9記載の発明に係る計算機の資源利用方式は、請求項2記載の計算機の資源利用方式において、上記被プロテクトノードを接続MTとし、接続MTの接続数制限をサービスプロセッサに行わせることを特徴とするものである。

【0017】請求項10記載の発明に係る計算機の資源利用方式は、請求項2記載の計算機の資源利用方式において、上記被プロテクトノードを計算機クロック周波数とし、計算機クロック周波数の初期設定をサービスプロセッサに行わせることを特徴とするものである。

【0018】請求項11記載の発明に係る計算機の資源利用方式は、請求項2記載の計算機の資源利用方式において、上記被プロテクトノードをキャッシュメモリとし、キャッシュメモリの初期設定をサービスプロセッサに行わせることを特徴とするものである。

【0019】請求項12記載の発明に係る計算機の資源利用方式は、請求項1記載の計算機の資源利用方式において、個別の識別子を、書きかえ可能な不揮発性メモリに格納しサービスプロセッサの固有な手続きにより識別子を書換え可能としたことを特徴とするものである。

【0020】請求項13記載の発明に係る計算機の資源利用方式は、請求項1記載の計算機の資源利用方式において、少なくとも上記識別カードの識別子および管理データテーブルの内容のどちらか一方を更新できることを特徴とするものである。

【0021】請求項14記載の発明に係る計算機の資源利用方式は、請求項1記載の計算機の資源利用方式において、上記識別カードを、サービスプロセッサとの特別な通信手段を有する専用不揮発性記憶媒体カードとしたことを特徴とするものである。

【0022】請求項15記載の発明に係る計算機の資源利用方式は、請求項1記載の計算機の資源利用方式にお

6

いて、識別カードとサービスプロセッサ間を独自のインタフェースにより接続したことを特徴とするものである。

【0023】

【作用】請求項1記載の発明においては、識別カードを使用して資源の利用範囲を決定することができるので、あらかじめすべてのH/WおよびS/Wを納入しておきながらも、識別カード内で許可された利用範囲だけをユーザに使用させることができる。つまり、H/WおよびS/Wの納入媒体は1種類のものだけ用意すればよく、納入も1度ですむ。

【0024】請求項2記載の発明においては、計算機の起動時に、管理データテーブルの内容を読み出すので、常に識別カードの内容を反映させたシステム構成の決定ができる。また、計算機の起動時に、識別カードで保証された管理データテーブルの内容に従ったオペレーティングシステムのインストールができる。

【0025】請求項3記載の発明においては、計算機の起動時に、識別カードから読み出した管理データテーブルの内容をメモリーに記憶させ保持するので、サービスプロセッサは起動要求のたびに識別カードの読み込みのためのアクセスを行う必要がない。また、サービスプロセッサは、被プロテクトノードの起動要求に対して、その被プロテクトノードの起動の可否を決定するので、それぞれの被プロテクトノードを独立して、許可の対象とすることができる。また、識別カードの更新/メンテナンス等の時、システムからカードが取りはずされた時でも、アプリケーションプログラムのロードができるようになる。

【0026】請求項4記載の発明においては、被プロテクトノードがオペレーティングシステムのもとで動くアプリケーションプログラムであるとき、オペレーティングシステムの中のセキュリティ管理マネージャが、管理データテーブルを参照し、アプリケーションプログラムの起動の可否をチェックし、そのアプリケーションプログラムのロードの許可を与えるので、識別カードの管理データテーブルの内容通りに各アプリケーションプログラム毎に許可の可否を決定することができる。

【0027】請求項5記載の発明においては、被プロテクトノードが、計算機に接続される端末（ワークステーション、パーソナルコンピュータ等）であるとき、サービスプロセッサは、管理データテーブル内の情報を用いて、その端末の利用の可否を決定する。

【0028】請求項6記載の発明においては、被プロテクトノードが、計算機に接続されるディスク記憶装置であるとき、サービスプロセッサは、管理データテーブル内の情報を用いて、そのディスク記憶装置の利用の可否を決定する。

【0029】請求項7記載の発明においては、被プロテクトノードが、計算機に接続される主記憶装置であると

き、サービスプロセッサは、管理データテーブル内の情報を用いて、その主記憶装置の利用の可否を決定する。

【0030】請求項8記載の発明においては、被プロテクトノードが、計算機に接続されるデータベースプロセッサであるとき、サービスプロセッサは、管理データテーブル内の情報を用いて、そのデータベースプロセッサの利用の可否を決定する。

【0031】請求項9記載の発明においては、被プロテクトノードが、計算機に接続されるテープ装置であるとき、サービスプロセッサは、管理データテーブル内の情報を用いて、そのテープ装置の利用の可否を決定する。

【0032】請求項10記載の発明においては、被プロテクトノードが、計算機に利用される計算機クロック周波数であるとき、サービスプロセッサは、管理データテーブル内の情報を用いて、その計算機クロック周波数の利用の可否を決定する。

【0033】請求項11記載の発明においては、被プロテクトノードが、計算機に接続されるキャッシュメモリであるとき、サービスプロセッサは、管理データテーブル内の情報を用いて、そのキャッシュメモリの利用の可否を決定する。

【0034】請求項12記載の発明においては、計算機毎に個別である識別子を書き換え可能としたことにより、識別子が何も書き込まれていない計算機を出荷し、導入時に識別カードと同期をとって識別子を設定することが可能となる。

【0035】請求項13記載の発明においては、識別カードの内容の更新に際して、遠隔地からの通信手段によって計算機を介して識別子や管理データテーブルの内容を更新することができるので、新たなS/WやH/Wの使用に対する識別子や管理データテーブルの内容の更新時に客先に出向がなくともよい。また、遠隔から識別カードの不法改ざんや不正使用の監視が行え、二重のチェックとなる。

【0036】請求項14記載の発明においては、識別カードを、プロセッサ内蔵型のICカードとして、ICカード内のプロセッサによりICカード内の情報をプロテクトすることができる。

【0037】請求項15記載の発明においては、プロセッサ内蔵型のICカードでなく他の価格の安い媒体カードを利用可能する場合でも、識別カードとサービスプロセッサ間を独自のインタフェースとしたことにより、容易にデータにアクセスされないというセキュリティ機能を持たせることができる。

【0038】

【実施例】

実施例1. まず、図1を用いて、この実施例の概略について説明する。図1はこの発明の一実施例のブロック図である。1は識別カード、2は被プロテクトノードを記述した管理データテーブル、3はセキュリティ管理プロ

グラム、4は被プロテクトノード、5は計算機筐体に設けられた個別の識別子、6は識別カードリーダー/ライタ、7はSVP（サービスプロセッサ）、8は中央処理装置、9は遠隔地計算機、10は計算機本体、11は公衆回線である。

【0039】識別カード1には被プロテクトノードを記述した管理データテーブル2とセキュリティ管理プログラム3が格納されている。管理データテーブル2には、被プロテクトノード4（オプションのH/W、及びS/W）の使用可否、及び使用期限等のデータが入っている。また、識別カード1内には、データの不法読み取り、不法改ざん防止の為、セキュリティ管理プログラム3が用意されており、SVP7は管理データテーブルへのアクセスの際、識別カード1に固有の識別子を送らなければならない。識別カード1はその識別子の整合がとれた場合だけ管理データテーブルへのアクセスを許可する。セキュリティ管理プログラム3とSVP7は識別子認証を行い、セキュリティ管理プログラム3は指定された識別子を送ってきた計算機に対してのみ識別カード1の管理データテーブル2のアクセスを許可する。

【0040】識別カード1の個別の識別子は計算機筐体に設けられた個別の識別子（たとえば、CPU-IDあるいは筐体番号）5と同一のものであり計算機据え付け時の起動で一回のみSVP7により識別カード1に書き込まれる。以降その個別の識別子がシステム立ち上げごとに認証に使用される。

【0041】この動作を図2を用いて説明する。システム立ち上げ時にシステムのコンフィグレーション或はイニシャルプログラムロードを行う際、筐体の識別子5、識別カードリーダー/ライタ6、被プロテクトノード4とインタフェースを持つSVP7は計算機筐体に設けられた個別の識別子5と識別カード1に格納された個別の識別子との認証をセキュリティ管理プログラム3を用いて行ない（S1）、整合がとれなければそこで、システム立ち上げを中止する（S7）。

【0042】整合がとれた場合（S2）、システムのコンフィグレーション或はオペレーティングシステムのイニシャルプログラムロードを行うが、SVP7はその時の被プロテクトノード4の使用可否（S3）、使用期限（S4）を識別カード1の管理データテーブル2を通して知り、認証された内容に従って、インストレーション或はロードの行う（S5）。このチェックを管理データテーブル2に定義されたすべての被プロテクトノードについて行い（S6）、システムを立ち上げる。

【0043】次に図3を用いて、OS（オペレーティングシステム）41のもとで動くアプリケーションプログラム42a～42nが起動される場合のチェックについて説明する。SVP7を通して、識別カード1内の管理データテーブル2との照合がオペレーティングシステム内のユーザプログラムセキュリティ管理マネージャ41

aによって行われ、許可されている場合はそのまま起動され、許可されていない場合は起動を中止される。また、SVP7は遠隔地との通信機能を持つ。遠隔地計算機9は、公衆回線11を通して遠隔地からの通信により、識別カード1へアクセスし、管理データテーブル2の更新を行う。

【0044】次に、この実施例の詳細について、以下に説明する。なお、以下においては、識別カード1が、ICカードであり、識別子を筐体番号として説明する。さらに、前述したユーザプログラムセキュリティ管理マネージャ41aをSVC（スーパーバイザーコール）インタフェースのチェックシステムコールで起動できるレーチンとして説明する。

【0045】まず、システムの概要について述べる。

- ・CPU-ID（筐体番号）と対になったICカードがあり、正規のICカードがセットされなければシステムは基本的には立ち上がらない。

- ・OSがICカードに格納されている管理データテーブルを読み出し、その内容に従って被プロテクトノードとして記憶された資源の機能をユーザに使用させるかどうか制御する。OSが制御する主な内容は、以下のものである。

- 1) ICカードにあるOSバージョン名とのチェックによるシステムの立ち上げの可否。
- 2) ICカードにある使用を許可するS/WとのチェックによるS/Wの起動の可否。
- 3) ICカードにあるシステムS/Wの利用可能な有効期限とのチェックによるシステムS/Wの立ち上げまたは起動の可否。
- 4) ICカードにある「同時に使用できる最大端末台数（あるいは、TCP/IPの論理リンク数）」とのチェックによる端末接続の可否。
- 5) ICカードにある製品クラス情報にもとづく、製品クラスのチェック。
- 6) ICカードにあるS/WのバージョンとのチェックによるS/Wの立ち上げまたは、起動の可否。

【0046】これらは、S/Wの不正使用を防止する目的で行うが、6)は他システムからのモジュールの不正なコピー防止を目的とするものである。このシステムでは、すべてのメーカ標準S/Wが、MT（マグネティックテープ）あるいは、DAT（デジタルオーディオテープ）に格納された状態で客先へ出荷される。客先では、その内容物すべてを、OS専用領域を持つディスクヘインストールする。OS専用領域は、MT内あるいはDAT内のS/W類、スワップ/ダンプ領域、および、各S/W独自に必要なとするディレクトリを含み、将来性を考えた十分な大きさを持ち、大きさは固定とする。このOS専用領域には、ユーザのプログラムやデータの格納を禁止する。

【0047】次に、ICカードのメモリ構造、および、

メモリに書き込まれる情報について述べる。

【メモリ構造】メモリにはフラッシュメモリ（またはEEPROM等でもよい）が使用され、図4に示すようにシステム領域とユーザ領域の2つに大別される。

【0048】【ICカードに書き込むデータ】システム領域には、ICカード自身の管理情報とユーザ管理情報が書き込まれる。

(1) PIN (Personal Identification Number)

10 PINは、利用者確認番号であり、この実施例では、システム設置後最初のIPL時にPINに筐体番号を設定し、次回以降のIPL時にPINを照合する。設定されたPINとICカードが装着されたマシンの筐体番号を照合することにより、1つのICカード内の情報（契約した資源を供給する情報）が特定のマシン以外では使用できないようにする。照合の結果が正しい場合には、ユーザ領域に設けられたADF (Application Data File) の内容に従って資源単体毎に動作可否が決定され、不正の場合には縮退モードでのシステム稼働となる。

(2) ICカード識別情報

ICカード識別情報とは、ICカードのH/W情報（メモリの種類や容量、ICカード自身のバージョン、ICカードのシリアル番号等）が書き込まれている。

(3) ユーザ管理情報

ユーザ（使用者）についての情報を管理するための領域であり、ICカード発行の際にユーザ情報が営業部門のユーザ管理D/B（顧客管理データベースとも呼ぶ）をもとに書き込まれる。ユーザ管理情報の内容は図5に示すとおりである。

(4) ADF (Application Data File)

ADFはICカードのユーザ領域をアクセスする際の1つの単位で、ユーザ領域を使用するためには、初めにADFを作成（指定されたADF-IDに対応する領域をユーザ領域に確保）しなければならない。ADFを作成する際には、APW (ADF毎のパスワード) とアクセス・レベルの指定が必要となる。

【0049】ユーザ領域では、ADF毎に分けて、メーカ側はADFの使用領域の管理とOSの核（カーネル）のもとで動くS/W（メーカ基本S/W）の管理を行い、ディーラではディーラ毎に決められた情報を管理する。以下、各管理情報毎に述べる。

(1) ADF毎の使用領域管理情報：各ADF毎の総バイト数と使用バイト数、空きバイト数の管理を行う。

(2) S/W管理情報：S/Wの管理を行い、S/W別の版名、使用開始日、有効期限、使用可否、製品クラス番号等の情報を管理する。図6を用いて具体的に説明する。図6において、ソフトウェアIDはソフトウェア毎の識別IDである。つまり、同一ソフトウェアはすべて

同じ識別子を持っている。その識別子はソフトウェアの種類毎に固有であり、同じソフトウェアであれば共通の識別子である。プロダクトコード、S/W名も同様である。一方、クラス、有効期限開始日、有効期限終了日等はユーザ固有の情報であり、そのユーザの契約内容を反映させた情報が書き込まれる。

【0050】以上述べてきた各情報を備えているのが管理データテーブル2であり、その論理的構成を図7に示す。

【0051】次に、計算機本体10のCPU-ID（筐体番号）の格納場所について説明する。本実施例においては筐体番号は、図8に示すように基本筐体内のSVPとCEパネル間に接続されている固有筐体アドレスボード内に格納されている。また、他の方式として不揮発性記憶媒体（例えばシステムディスク）の特定エリアにあってもよい。

【0052】次に、本実施例の資源利用方式におけるS/W管理について説明する。図9はS/W管理機能を実現する構成を示す概要図である。この図を用い、まずS/W管理機能の仕組みを説明する。

1) ベンダマシンからのICカード作成/変更について、図9及び図10を用いて説明する。

(1) 契約内容(S10)に従って、顧客データベースメンテナンス手段301を用い、顧客データベース303を生成/更新する(S11)。

(2) 次にS12において、ICカード作成手段302を用いて、更新された顧客データベース303からICカードの作成/変更を行う。ICカード作成手段302は、ICカードに関するSVCインタフェース306、カーネル304を用いてICカードのREAD/WRITE等を行う。

【0053】2) ユーザマシンでの動作について図9及び図11を用いて説明する。

(1) IPL時、他のイニシャライザプログラムにさきがけてICカードチェック手段307が実行され、ICカードに関して図11に示すフローに従ってチェックを行う。ICカードの内容に変更が生じた場合にはその都度チェックが必要となる。

(a) 特権フラグが設定されているか?(S20)
特権フラグはICカード内の情報ではなくOS内部に持つ情報である。このフラグを設定することにより、ICカードのチェックなしで全てのソフトウェアを動作させることができる。なお、この機能は非公開とする。

(b) 正常なICカードが装着されているか?(S21)

ICカードへのアクセスがエラーとなる場合(ICカードが装着されていない場合も含む)SVPディスク311に格納されている以前に記憶された管理データテーブルを読み込む(S23、S24)。SVPディスク311に管理データテーブルがない場合には最低限の機能を

実行できる縮退モードで立ち上がる(S23、S33)。SVPディスクの情報から立ち上がる場合には、そのファイルの生成日が調べられ、一定期間以上経過していた場合には縮退モードで立ち上がる(S25、S33)。

(c) ICカード内の管理データテーブルの読み込み(S22)

読み込む情報には以下のようなものがある。

読み込まれる情報: ユーザレベル、動作可能CPU台数、CPU-ID、OS名、OS版名(バージョン名ともいう)と有効期限、使用可能なS/Wの種類・版名・有効期限・製品クラスetc.

(d) 読み込んだ管理データテーブルの正当性チェック(S26)

ADFの持つAPW(ADF毎のパスワード)と照合するために、セキュリティ管理プログラムは、ICカードを使用してシステムを立ち上げようとするユーザにパスワードの入力を要求する。そしてセキュリティ管理プログラムは、コンソールから入力されたパスワードとAPWをチェックし、異なると判定された場合には縮退モードで立ち上がる。契約期限切れの近いS/Wに関しては、IPL時メッセージでその旨を通知する(S27、S28)。

(e) 読み込んだ管理データテーブルのメモリ上のICカード情報テーブル305への格納(S29)

前述した(d)のチェックがOKであった場合、ICカードから読み込んだ管理データテーブルをメモリ上のICカード情報テーブル305へ格納する。ICカード情報テーブル305はメモリダンプ等で解読されないよう暗号化する。また、前述した(b)の次のIPL時チェック(S21、S23)で使うため、ICカード内の管理データテーブルをSVPディスク311へ書き込む(S30)。

(f) IPL回数の加算(S31)

前述した(d)で正常と判断された場合には、メモリ上のICカード情報テーブル305のIPL回数に1加算する。

【0054】(2) ICカードチェック手段307の動作により正常なシステムと判断された場合通常のIPLが実行され、以後各S/Wはその起動時以下の方法によってOSによる起動時チェックを受け、契約S/Wのみが動作する。その機能の動作時必ず実行されるモジュール(IPL時イニシャライザ等)の動作の先頭で、OSが提供するSVCインタフェース306のチェックシステムコールを呼ぶ。それがノーマルリターンした場合以外はエラー終了させる。SVCインタフェース306のチェックシステムコールは、引数としてその製品のコード、版名等をもらい、ICカード情報テーブル306と照らし合わせ、動作可/不可、製品クラス等を返す。また、起動回数をカウントしたいS/W製品に関しては、

その意志を伝える引数も渡す。これにより、IPL後シャットダウンするまでの起動回数がメモリ上に記録され、シャットダウン時、それがICカード上の管理データテーブル中の累積起動回数に加算される。

【0055】(3) ICカードの管理データテーブルをモニタする管理データテーブルモニタ機能310(図9参照)を提供し、ユーザレベルでどのソフトウェアが動作可能かを確認できるようにする。

【0056】次にアプリケーションプログラムからのSVCインタフェース306のチェックシステムコール(ischged)について説明する。各S/Wは、メインとなるモジュールおよびn個のサブモジュールから構成されている。図12にS/Wの関係を表すブロック図を示す。S/Wはメインとなるモジュールが起動された直後本システムコールを呼び出し、リターン値を受け取る。OSによるICカード情報テーブルとのチェックを行い、そのリターン値が正常値である場合のみ動作を続行し、エラーリターンした場合にはその旨をメッセージ出力し、アボートさせる。ここまでの処理の流れを図13に示す。本システムコールが呼び出される箇所は、

- 1) イニシャライザ、ユーザから直接呼び出せるロードモジュールの先頭等、その箇所でアボートすることにより、その機能が使い物にならない箇所であること、
- 2) アボートしたことをユーザが気付き易い箇所であること、
- 3) コール回数が必要最小限であること。起動回数をカウントする必要があるものは、その値が意味のあるような箇所であること、という条件を満たさなければならない。

(1) チェックシステムコールのコーリング・シーケンスは、たとえば、以下のようなものである。

```
#include<charge.h>
int  ischged(prdctcd, version, classp, cntreq);
int  prdctcd; /* 製品コード */
char *version; /* 製品のバージョン */
int  *classp; /* 製品クラス値へのポインタ */
int  cntreq; /* 起動回数カウント要求フラグ */
int  nomsg; /* メッセージ不要フラグ */
```

(2) チェックシステムコールの機能について説明する。prdctcdで指定された製品コードのversionで指定された版の製品が、そのシステムにおいて起動が許されているかどうかをチェックする(各S/Wにおいて自らの製品コードおよびバージョンを指定する)。製品クラスのある製品は、classpを指定してやり、正常リターン時に返されるクラス値に応じた動作をする。製品クラスのない製品ではNULLを指定す

る。cntreqにNEED_COUNT(=1)を指定すると、本SVCの処理の中で、その製品の起動回数が1加算される。その情報はシャットダウン時、ICカード内の累積起動回数に加算される。これにより、その製品の使用頻度を知ることができる。起動回数をカウントする必要のない場合にはNULLを指定する。prdctcdおよびversionで指定できる値およびclasspに返される値については、charge.hに定義されている。通常ischgedはエラー検出時エラーメッセージを起動端末に出力するが、これが不要な場合にはnomsgにNOMSG(=1)を指定してやる。

(3) チェックシステムコールのリターン値は以下のとおりである。

起動を認められている・・・0

起動を認められていない(非契約)・・・1

起動を認められていない(契約期間外)・・・2

エラー終了した・・・-1

【0057】次に被プロテクトノードがH/Wの場合について説明する。この実施例においては、図5に示すように、管理データテーブル内のユーザ管理情報にその計算機システムにおいてOSがサポートできるH/Wの制限数あるいは制御量に関する情報が記述されているものとする。SVPはまた、計算機の持っている日付が、ユーザ管理情報の中の使用開始可能日と有効期限の間であることを確認する。もし有効期限の間でなければ以降のチェックは行わない。システムの立ち上げ時に、サービスプロセッサはH/Wの制限数あるいは制御量に関する情報を参照する。また、サービスプロセッサは、その計算機に接続されている各H/Wの構成を独自のやりとりによって確認する機能を有している。そして、確認したH/Wの台数を記憶するレジスタを有し、そのレジスタに書き込まれた台数とユーザ管理情報内の制限数を比較し、制限数の範囲内であれば、そのH/Wを正式にこれから立ち上げる計算機のシステム構成に加えて、IPLを行う。例えば、ユーザ管理情報において制限されたワークステーション台数が3台(まで)と記述されているとき、実際に物理的に接続されているワークステーションが2台であったとき、その2台のワークステーションは論理的にも計算機に接続が許可され、使用可能となる。また、物理的に接続されているワークステーションが3台であっても、ユーザ管理情報において記述されている台数以内、すなわち3台以内であるので、同様に接続が許可され、その計算機において使用可能となる。

【0058】次に、物理的に接続されているワークステーション台数が4台以上であった場合を説明する。この場合、最初の3台までは接続が許可されるが、4台目以降のワークステーションは物理的に線はつながっていても、計算機のシステム構成には含まれない。ここで、最初の3台というのはSVPによって認識される順序によ

るので、どのワークステーションが接続不可となるのかはSVPに依存している。ここではワークステーションを例にとって説明したが、台数で数えられるH/Wに関しては同様に判断される。すなわち、FXD（固定ディスク）、データベースプロセッサ、MTなどである。

【0059】次に、被プロテクトノードが主記憶装置である場合について述べる。主記憶装置がメモリーボード単位で数えられるとき、その数によって前述したように計算機での使用を制限することができる。また他の方法として、実装されている全てのメモリーに一連のアドレスがふられているときは、使用可能なアドレス範囲情報を指定することによって、その識別カードを持つユーザに許可されている容量を使用可能とするやり方でもよい。また、この2つの方式は被プロテクトノードがキャッシュメモリで、ハード的に設定されている場合にも適用可能である。つまりキャッシュメモリに割り当てるメモリーボードを枚数で制限する方法と、キャッシュメモリ用として使用するメモリーのアドレスを指定する方法である。あるいは、キャッシュメモリがソフト的に実現されている場合には、キャッシュメモリ管理用のソフトウェアを本方式のS/W管理の対象としておくことによって、使用を制限することも可能である。さらにこれらの方式を組み合わせることによって、全ての整合性がとれた場合のみ、実際にキャッシュメモリを使用可能とする方法も有効である。

【0060】次に、被プロテクトノードが計算機クロック周波数であった場合について述べる。これにはシステム立ち上げ時にパラメータを受け取ることによって、指定されたクロック周波数を発生させる手段が計算機にあらかじめ備えられていることを前提としている。計算機はSVPによって管理データテーブルからユーザに許可されたクロック周波数を受け取り、そのクロック周波数で稼働する。

【0061】以上のように、この実施例に係わるプログラムロード方式及び周辺機器インストール方式計算機は計算機筐体に設けられた個別の識別子とその計算機にオプションとして接続されるH/W、或はその計算機上で動作するS/Wを、識別カードおよびSVPにより、カード内に記録された被プロテクトノードを記述した管理データテーブルのデータに従って認証させ、それらの接続あるいは起動を制限するものである。

【0062】本実施例においては、認証用の識別カードは当該計算機に対し一枚しか存在せず、それぞれ対応する一台の計算機においてでしか機能しないので、識別カードの対象計算機が限定されることによって、その計算機で使用されるS/Wあるいは周辺機器の制限情報は確実に固有のものとなり、セキュリティ効果は増大する。また、識別カードを使用することより、その中へ格納する被プロテクトノードを記述した管理データテーブルのデータを不法に読取、改ざんされる危険を防止する。そ

してその対象を動作するプログラムのみではなく、接続されるH/Wコンフィグレーション情報まで広げることにより、容易なモデルレパートリの拡張を実現する。またSVPに識別カードとのインタフェースを設けることにより、既存の基本処理装置、各周辺機器コントローラは変更する必要はなく、容易にシステムに組入れる事ができる。更にSVPを経由して遠隔地から識別カードのアクセスを可能にすることにより、被プロテクトノードを記述した管理データテーブルの読取、更新を遠隔地から行うことを可能にする。

【0063】この実施例の利点として、以下のようなものがあげられる。

- ・より万全なセキュリティシステムの提供。
- ・必要な機能だけ購入できるOS分の分割化。
- ・S/Wの試使用精度等の新しいサービスの提供。（遠隔運用保守システムと連携した場合）
- ・SE作業の省力化。
- ・ディーラS/Wの不正使用防止対策を支援。
- ・S/W製品の契約による売上の確保。
- ・保守性向上。
- ・出荷作業の省力化。
- ・ロイヤリティ支払いの適正化。
- ・メーカーによる顧客管理の実施。

また、この実施例によれば、システムの不正使用の防止をはかることができる。また、顧客管理システムを導入することにより、ユーザ登録制度を実施し、メーカーでも顧客管理ができる。

【0064】実施例2. 図14を用いて他の実施例を説明する。図14はこの発明におけるユーザ管理情報の別の例である。実施例1において、ワークステーションの接続台数を制限する例を説明したが、単に台数のみのチェックでなく、接続可能なモデルを制限するようにしてもよい。すなわち、モデルコードを管理データテーブルに設定しておき、ワークステーションから読み取ったモデルコードと比較して、一致した場合のみ接続を許可する方式でもよい。さらに、モデルコードを一致させたうえで台数も制限するという方式でもよい。この場合のユーザ管理情報中には前述した項目に加えて、ワークステーションのようにモデルコードを有する被プロテクトノードについては、被プロテクトノード毎に有効なモデルコードを記述する項目も設定しておく。具体的には図14に示すように、実施例1で使用したユーザ管理情報にモデルコードに関する項目を追加する。なお、このモデルコードの設定は必要に応じて、それぞれの被プロテクトノード毎に複数設定してもよい。具体的には1項目についてモデルコードを配列のように並列的に複数書いてもよいし、ワークステーションモデルコード1、ワークステーションモデルコード2、・・・nのように項目を複数にしてもよい。サービスプロセッサは設定されている書式に沿って、必要な情報を読み取れるようあらかじ

め知らされているものとする。

【0065】実施例3. 次に図15を用いて他の実施例について説明する。この図では、図7に示した管理データテーブルの構成に、さらに、接続H/W管理情報をあわせ持つ。この実施例においては、管理データテーブル中に接続H/W管理情報を持つ。前述したS/W管理情報と同様に、被プロテクトノードである各H/Wは、それぞれH/Wのカテゴリーを識別する被プロテクトノード識別子を有している。その被プロテクトノード識別子毎に1つの接続H/W管理情報を使用する。接続H/W管理情報のデータフォーマットを図16に記す。図16に示すように、接続H/W管理情報は図5に示したユーザ管理情報のH/Wに関する項目を別個独立に持つものである。サービスプロセッサは、その計算機に接続されている各H/Wの構成を独自のやりとりによって確認する機能を有しており、H/W確認時に、サービスプロセッサは、そのH/Wの被プロテクトノード識別子を受け取り、その情報をもとに、該当する接続H/W管理情報を参照する。この時、SVPはその被プロテクトノードの登録日と使用有効期限を計算機の持つシステム日付と照合し、有効でなければその被プロテクトノードの接続を許可しない。また、SVPは確認したH/Wの台数を記憶するレジスタを有し、そのレジスタに書き込まれた台数と参照した接続H/W管理情報内の最大接続台数を比較し、その制限数の範囲内であれば、そのH/Wを正式にこれから立ちあげる計算機のシステム構成に加えて、IPLを行う。具体的な判断の流れについては、実施例1と同様であるので説明を省略する。実施例1との違いは参照する情報の書かれている場所が接続H/W管理情報内であるということである。

【0066】なお、実施例1と同様に、ワークステーションだけでなく、台数で数えられるH/Wに関しては上述した例と同様に、接続H/W管理情報を参照して、システム構成への包含の可否が判断される。すなわち、FXD、データベースプロセッサ、MTなどのシステム構成への包含の可否が判断される。

【0067】また、主記憶装置がメモリーボード単位で数えられる時や、キャッシュメモリ用として使用するメモリーボードを枚数で制限する場合もこの方式を適用できる。また、接続H/W管理情報のレイアウトを図17のようにすれば、メモリーボードの枚数でない方法で、使用許可の制限を行う場合にも適用できる。図17(a)は被プロテクトノードが主記憶装置の場合である。図17(b)は被プロテクトノードがキャッシュメモリの場合である。図17(c)は被プロテクトノードが計算機クロック周波数の場合である。例えば、実装されている全てのメモリーに一連のアドレスがかかれているときは、図17(a)のLIMITINFO(使用可能アドレス範囲情報)をSVPが参照し、許可されているメモリ容量をその識別カードを持つユーザに対して使用可能とす

る。また、被プロテクトノードがキャッシュメモリであるとき、図17(b)に示すようにLIMITINFO(キャッシュメモリ割当アドレス範囲情報)をSVPが参照し、指定されているアドレスの範囲をキャッシュメモリとして使用可能にする。また、被プロテクトノードが計算機クロック周波数であった場合、図17(c)に示すようなLIMITINFOには使用可能周波数クロック情報が記述されており、SVPはそのユーザに許可されたクロック周波数情報を使用して、計算機をそのクロック周波数で稼働させる。この場合も実施例1と同様に、システム立ちあげ時にパラメータを受け取ることによってそのパラメータに応じてクロック周波数を可変的に設定できる手段があることを前提としている。以上のようにこの実施例においては、被プロテクトノード毎に接続H/W管理情報を識別内の管理データテーブルに持つことによって、被プロテクトノードを必要に応じて、個別に任意の使用許可条件を設定できる。

【0068】実施例4. 次に、被プロテクトノードを台数や容量でのみでなくH/Wのモデルコード毎に接続を制限する他の実施例について説明する。この実施例においては、図18に示すように、接続H/W管理情報の中にモデルコードとそのモデルコード毎の最大接続数を記録しておく。また、前述した実施例と同様、接続H/W管理情報と計算機の持つ日付のチェックも行われるものとする。これは以降の実施例全てにおいて共通であるので以降説明を省略する。実施例1, 2と同様に被プロテクトノードがワークステーションである場合を例にとる。SVPはシステム立ち上げ時に、物理的に接続されているワークステーションからモデルコードを読み取り、接続H/W管理情報中に設定されているモデルコードと比較して、一致している場合のみ論理的にも接続を許可し、システム構成に加える。最初に書かれているモデルコードと一致しなければ、2番目のモデルコードと比較し、一致していれば接続を許可する。ここでも一致しなければ、3番目のモデルコードと比較する、というように、SVPは1つのワークステーションに対して一致するまですべてのエントリーとの比較を繰り返し、n個目のモデルコードも不一致であった時は、そのワークステーションに対しては接続を許可しない。そして、SVPは次のワークステーションまたは他のH/Wのチェックを続行する。ワークステーション以外の他のH/Wについても、チェックの手順は同様である。モデルコードを有するH/Wであれば、この方式は適用可能である。ここでは、モデルコードのみを比較する例で説明しているが、この場合モデルコード毎の最大接続数にはNULLが入っているものとする。

【0069】実施例5. 次に実施例4と同様に図18に示す接続H/W管理情報を用いて、モデルコードだけでなく接続台数の制限を行う場合について説明する。この実施例においては、実施例4とは異なりモデルコード毎

の最大接続数には、実際に接続を許可する有効な数字が入っているものとする。さらに SVP は被プロテクトノード毎、モデルコード毎に接続を許可された H/W の台数を記憶するレジスタを有しているものとする。SVP は実施例 4 と同じ手順で物理的に接続されているワークステーションのモデルコードと一致するモデルコードがエントリに存在するかどうか探し、なければ論理的な接続を許可しない。もしあれば、チェック中の被プロテクトノードのモデルコードの同じ接続数が記憶されているレジスタの値を参照し、その値に 1 を足した数値がモデルコード毎の最大接続台数以下であるかどうかチェックする。そして、そのチェックが OK であれば、論理的な接続を許可する。チェックが OK でなければ、モデルコードが一致しても接続は許可されない。

【0070】実施例 6. また他の実施例として、前述した実施例とは異なるレイアウトを持つデータフォーマットを示す。この実施例において使用する接続 H/W 管理情報のデータフォーマットを図 19 に示す。図に示すように、この実施例で使用する接続 H/W 管理情報には被プロテクトノードである H/W 1 台毎に固有な識別子（たとえば、端末 ID やネットワーク ID など）を記述する複数の項目がある。そして個々の H/W も 1 台毎に固有な識別子を記憶する手段を有しているものとする。SVP はシステム立ち上げ時に H/W から読み取った識別子と接続 H/W 管理情報から読み取った識別子を比較し一致した場合のみ接続を許可する。この場合も前述した実施例同様先頭の ID と不一致でも、SVP は 2 番目、・・・ n 番目までというように一致するまでサーチし、いずれかで一致すれば接続を許可するものとする。さらに、最大接続台数も記述しておき、識別子と二重にチェックしてもよい。

【0071】以上のように、この実施例では、被プロテクトノードが持っている固有の識別子情報を資源利用に活用し、顧客に納入することが確定した被プロテクトノードとなる H/W の識別子を、識別カードの管理データテーブルにあらかじめ書き込んでおくことにより、計算機の識別子との照合だけでなく被プロテクトノードの識別子の照合も行い、より厳重にチェックする方法を提供する。

【0072】実施例 7. 実施例 1 においては、S/W 管理情報の中の、S/W-ID は S/W 毎に個別だがユーザ毎、S/W 毎に固有な ID としてもよい。ユーザは自分用に設定された固有の S/W-ID を持つ識別カードを使用しない限り、計算機の立ち上げ時に S/W をロードすることができない。また、起動回数は S/W の種類によって、実際にユーザが起動した回数を記録してもよい。さらに、ユーザが起動できる最大起動回数を保持する項目を設定し、ユーザの S/W の起動を有効期限だけでなく累積回数で制限してもよい。

【0073】実施例 8. なお、実施例 1 においては、識

別カードの識別子は計算機据付け時の起動で一回のみ SVP 7 により識別カード 1 に書き込まれるが、必要に応じて、任意のタイミングで書き換えを行ってもよい。また、この書き換えは、例えば、公衆回線等を介して遠隔地から行ってもよい。

【0074】実施例 9. 管理データテーブルの書き換えは計算機システムのオンライン稼働中も実行可能である。新たに書き換えられた管理データテーブルの情報を利用して計算機を稼働させるためには再度 IPL を行えばよい。また、IPL をやり直すのではなくコマンドを使用して IC カード情報に従ってシステムの再構成及び S/W のロードを行うようにしてもよい。

【0075】実施例 10. 筐体番号は導入時客先で書き込んでもよい。あるいは事前に書き込んだものを識別カードと 1 対にして導入してもよい。筐体番号を、出荷時には固有筐体アドレスボード内に格納せず、据付け後に書き込むことも可能である。

【0076】実施例 11. 計算機筐体に設けられた個別の識別子 5 を、筐体のマザーボード上の EEPROM に記憶させ SVP 接続のコンソールにより、識別子を書換え可能としてもよい。オペレータは、パスワードにより筐体番号変更画面を開き識別番号を書換える。

【0077】実施例 12. 識別カードを、プロセッサ内蔵型 IC カードではなく、カード内部にセキュリティ管理プログラム 3 を持たないものとしてもよい。図 20 において、12 はセキュリティ管理プログラム 3 を持たない識別カード、2 は被プロテクトノードを記述した管理データテーブル、14 はセキュリティ管理プログラム、4 は被プロテクトノード、5 は計算機筐体に設けられた個別の識別子、17 は識別カードリーダ/ライタ、7 は SVP、8 は中央処理装置、9 は遠隔地計算機、10 は計算機本体、11 は公衆回線、23 はインタフェース用専用 H/W、24 は 8 ビットのデータバス、25 は 1 ビットの制御線である。本実施例では SVP 7 内にセキュリティ管理プログラム 14 を持たせ、識別カード内の管理データテーブルのセキュリティは、SVP 7 とのデータ通信手順によって守られる。このとき、識別カードリーダ/ライタ 17 と SVP 7 間をインタフェース用専用 H/W 23 を介し 8 ビットのデータバス 24 と 1 ビットの制御線 25 で結ぶ。SVP 7 と識別カード 12 とのデータ通信はインタフェース用専用 H/W 23 を通して行われる。SVP 7 は識別カード 12 にアクセスする時、まず識別カード 12 の識別アドレス 8 ビットをデータ線 24 を通して送る。その後規定時間後に 1 ビットの制御線 25 にリードかライトかの情報を乗せ、データバス 24 を介してデータのアクセスを行う。SVP 7 では、セキュリティ管理プログラム 14 によって事前に被プロテクトノード 15 からの識別子を認証し整合が取れたときだけ、識別カード 12 内の管理データテーブル 2 の情報に従い、被プロテクトノード 4 の起動を行う。

【0078】この実施例は、識別カード12にセキュリティ管理プログラムがない場合、すなわち単に管理データテーブル13のみが存在している場合、識別カード内のデータを不正に読み取られたり不正に改ざんされたりされ易くなることを考慮したものである。すなわちICカードのようにセキュリティ管理プログラムを内蔵することができる識別カードの場合には、識別カード自体がプロテクトされているのに対し、この実施例のように、識別カードが単に情報のみを記憶している場合には、この識別カードをアクセスする場合のインタフェースをメーカー独自のものとする事によりセキュリティの機能を向上させようとするものである。従って、この実施例では、標準化されたインタフェースを故意に持たず、一般には知られていない固有のインタフェースを提供する。このようにして、識別カードが単に情報を保持する場合であっても、識別カードへのアクセスを限られたシステムのみが行えるようにするものである。

【0079】

【発明の効果】本発明は以上説明したとおり、使用される計算機ハードウェアと使用されるオプションH/W或は計算機ソフトウェアが一对一に限定されるためオプションH/W或は計算機ソフトウェアの不法な使用が防止される。また、ユーザプログラム記憶媒体には、不正防止のためのハードウェアの固有識別子を格納する必要がないので出荷形態が簡素化される。また、ユーザプログラム記憶媒体には、固有識別番号を格納する必要がないので異なったハードウェアへのインストールが自由に行える効果がある。オプションH/W或はソフトウェアの追加販売が識別カード内管理データテーブルの更新のみで可能になるので販売、出荷手続きが簡素化され、出荷媒体には全てのソフトウェアを格納できるので、媒体の出荷形態が簡素化される効果がある。

【0080】また、請求項2記載の発明によれば、サービスプロセッサが識別子の照合を行うのでサービスプロセッサに変更を加えるだけで前述したような方式を容易に達成することができる。

【0081】請求項3記載の発明によれば、管理データテーブルを計算機側に記憶してしまうので、起動要求時の識別カードへのアクセスが不要となり、システムからカードがはずされていてもシステムに影響がなく、識別子の比較を即座に任意の時点で行うことができる。

【0082】請求項4記載の発明によれば、ソフトウェアを起動する場合にセキュリティ管理マネージャをオペレーティングシステムに備えておくことにより、アプリケーションプログラムの起動要求に対する可否を徹底することができるので、オペレーティングシステムに対してセキュリティ管理マネージャを追加するという最小限の変更でアプリケーションプログラムの制御を行うことができる。

【0083】さらに請求項5～11記載の発明によれ

ば、オプションH/Wのインストール形態が識別カードの内容により一意的に決るので、モデル毎、或は契約毎に、H/Wの差別化をする必要がなくなるという効果がある。

【0084】請求項12記載の発明によれば、計算機の識別を控え可能にしたので、計算機の製造時、出荷時、イントール時、その他任意の時点で識別子を容易に書きかえることができる。

10 【0085】請求項13記載の発明によれば、識別カードの識別子、あるいは、管理データテーブルを更新できるようにしたので、遠隔地からでも識別カードを更新することが可能になる。さらに、場合によっては、遠隔から識別カードの不法改ざんや不正使用の監視が行え、二重のチェックとなる。

【0086】請求項14記載の発明によれば、識別カードにプロセッサ内蔵型ICカードを使用することにより管理データテーブルの不法改ざんの抑止効果を向上させる効果がある。

20 【0087】また、請求項15記載の発明によれば、識別カードにプロセッサ内蔵型ICカードでなくSVPとの固有なインターフェースを持つ不揮発性記憶媒体カードを使用する事によっても同様の効果を持つ。

【図面の簡単な説明】

【図1】この発明の実施例1を示すブロック図である。

【図2】この発明におけるシステム立ち上げ時チェックの流れ図である。

【図3】この発明におけるアプリケーションプログラムの起動時の流れ図である。

30 【図4】この発明におけるICカードのメモリ構造を示す図である。

【図5】この発明におけるユーザ管理情報を示す図である。

【図6】この発明におけるソフトウェア管理情報を示す図である。

【図7】この発明における管理データテーブルの構成を示すブロック図である。

【図8】この発明のソフトウェア管理機構のハードウェア構成図である。

40 【図9】この発明のソフトウェア管理機能概要図である。

【図10】この発明におけるICカード作成までの手順を示す流れ図である。

【図11】この発明におけるICカードチェック手段の手順を示す流れ図である。

【図12】この発明におけるS/Wの関係を示すブロック図である。

【図13】この発明におけるチェックシステムコールを呼び出す流れ図である。

50 【図14】この発明におけるユーザ管理情報を示す図である。

- 3 セキュリティ管理プログラム
- 4 被プロテクトノード
- 5 計算機筐体に設けられた個別の識別番号
- 6 識別カードリーダー／ライター
- 7 SVP
- 8 中央処理装置
- 9 遠隔地計算機
- 10 計算機本体
- 11 公衆回線
- 12 識別カード
- 14 セキュリティ管理プログラム
- 17 識別カードリーダー／ライター
- 23 インタフェース用専用H／W
- 24 8ビットデータバス
- 25 1ビット制御線

10

1 4 セキュリティ管理プログラム
1 7 識別カードリーダ／ライタ
2 3 インタフェース用専用H／W
2 4 8ビットデータバス
2 5 1ビット制御線

23 インタフェース用専用H/W
24 8ビットデータバス
25 1ビット制御線

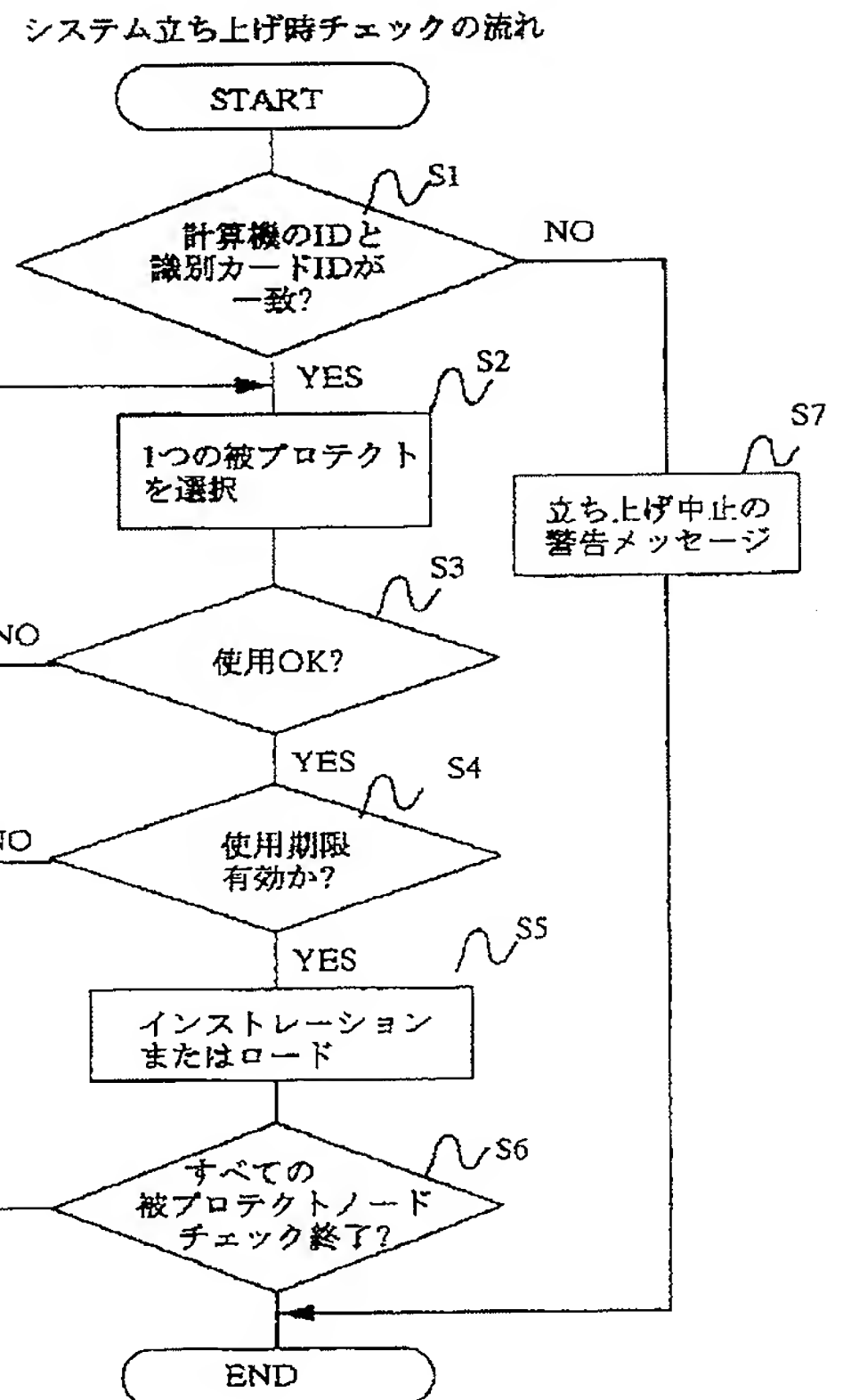
23 インタフェース用専用H/W
24 8ビットデータバス
25 1ビット制御線

23 インタフェース用専用H/W
24 8ビットデータバス
25 1ビット制御線

23 インタフェース用専用H/W
24 8ビットデータバス
25 1ビット制御線

- 23 インタフェース用専用H/W
24 8ビットデータバス
25 1ビット制御線

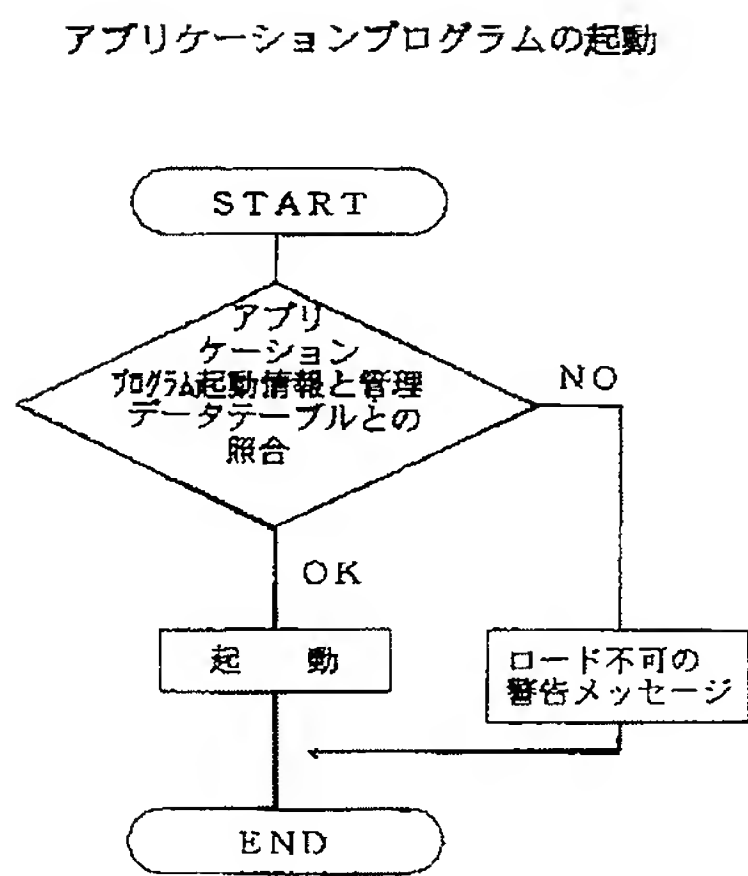
【図 2】



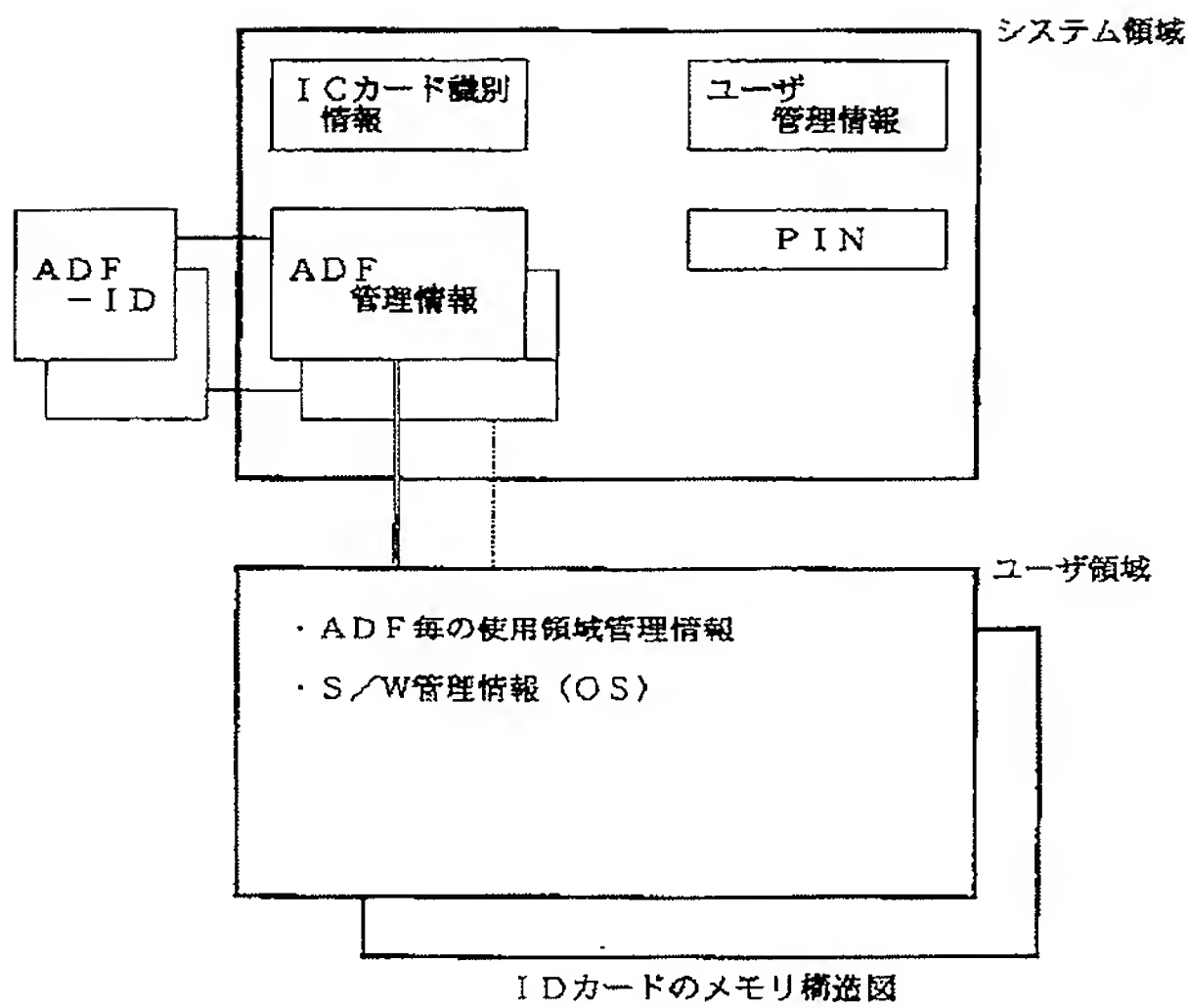
【図 16】

H/W-ID	H/Wのカテゴリ毎のID番号 (被マテクトード識別子)
STARTDAY	H/Wのカテゴリ毎の登録日
LIMITDAY	H/Wのカテゴリ毎の使用有効期限
LIMITNUM	最大接続台数

【図3】



【図4】



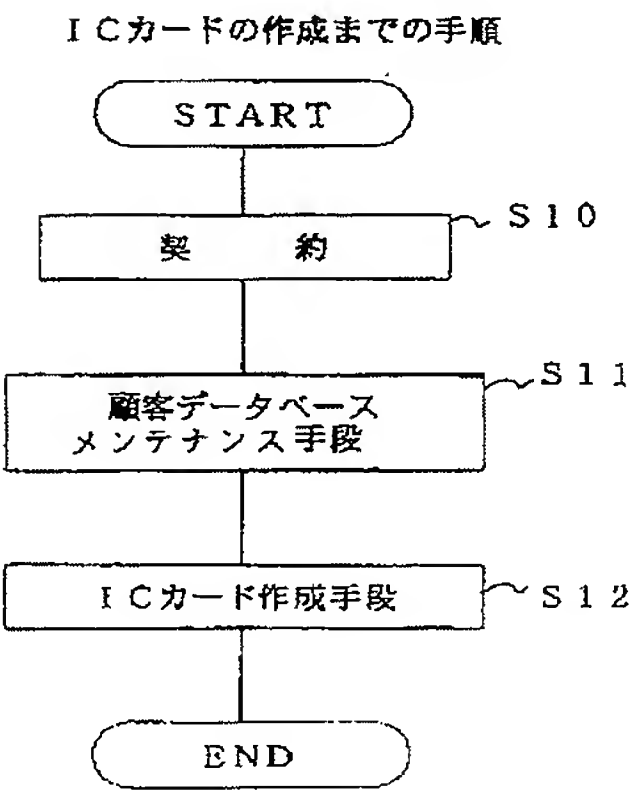
【図5】

ユーザ管理情報	
名称	説明
ディーラID	ディーラ識別ID
ユーザID	ユーザ識別ID
マシンID	機種/モデル識別ID
ユーザレベル	システム使用者識別レベル
使用開始可能日	ICカードの使用開始可能日
有効期限	ICカードの使用有効期限
更新日	ICカード内データの最終更新日
ディーラ名	ユーザレベルに対応するディーラ名
ユーザ名	システム使用者名
マシン名	機種/モデル名
CPU ID	CPU ID
OS名	OS名
OSバージョン名	OSバージョン名
ワークステーション台数	OSのサポートワークステーション台数
接続FDD台数	OSのサポートFDD台数
主記憶装置容量	OSのサポート主記憶装置容量
接続データベースプロセッサ台数	OSのサポートデータベースプロセッサ台数
接続MT台数	OSのサポートMT台数
計算機クロック周波数	その計算機で使用するクロック周波数
キャッシュメモリ設定情報	キャッシュメモリとして設定するメモリ容量
IPL回数	IPL回数

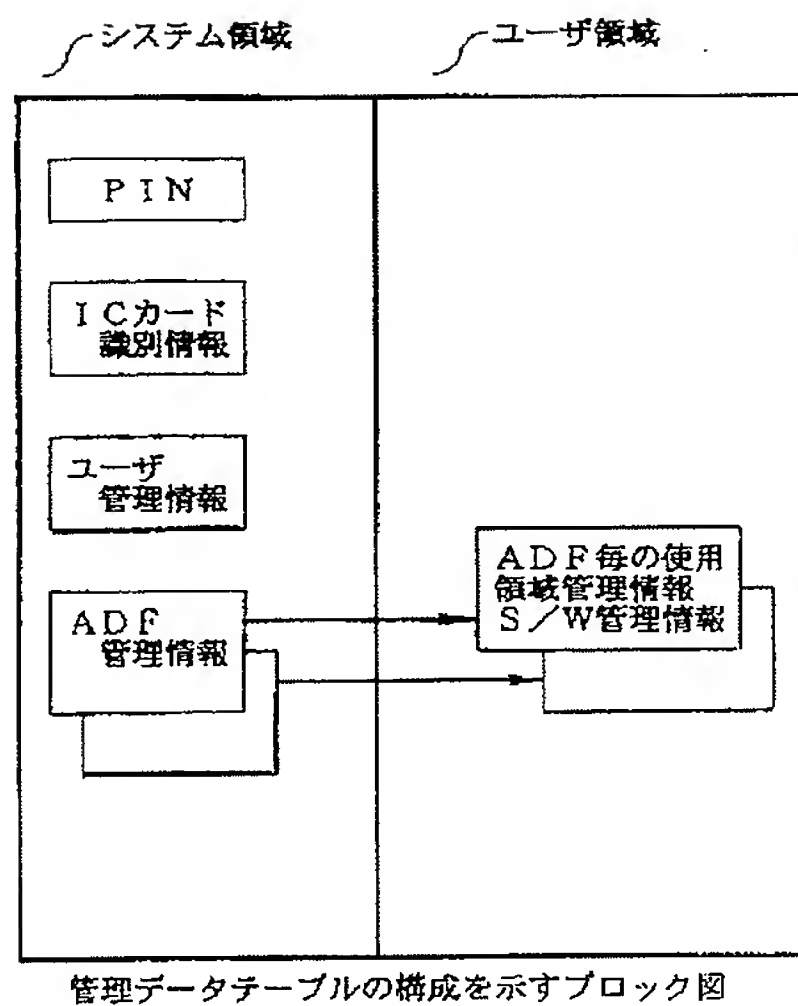
【図6】

S/W管理情報	
名称	説明
S/W ID	ソフトウェア毎の識別ID
加付コード	ソフトウェア毎の製品コード
S/W名	ソフトウェア毎の名称
クラス	製品クラス番号 (S/Wのポート・クライアント版) が入る。クラス番号が無い場合は、NULLとする。
有効期限開始日	S/W毎の登録日
有効期限終了日	S/W毎の使用有効期限
リクエストフラグ	起動回数カウント要求フラグ (ON: 1, OFF: 0)
起動回数	S/W毎の起動回数
バージョン	S/Wバージョン名
使用フラグ	使用不可フラグ (0以外で利用可能)
サポートフラグ	サポートフラグ (ON: 1, OFF: 0)
リリース	S/W毎のリリース・バージョン (無い場合はNULL)
メンテナンスフラグ	保守フラグ

【図10】

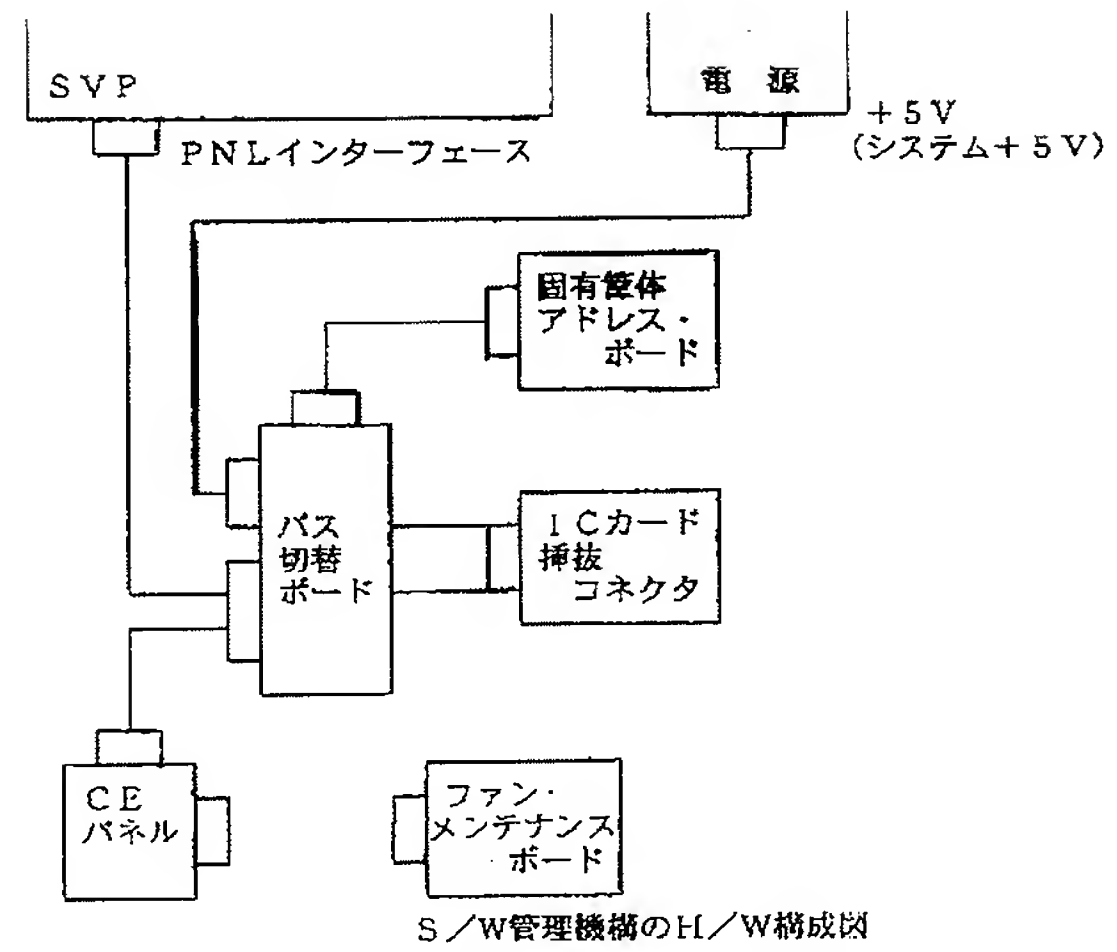


【図 7】



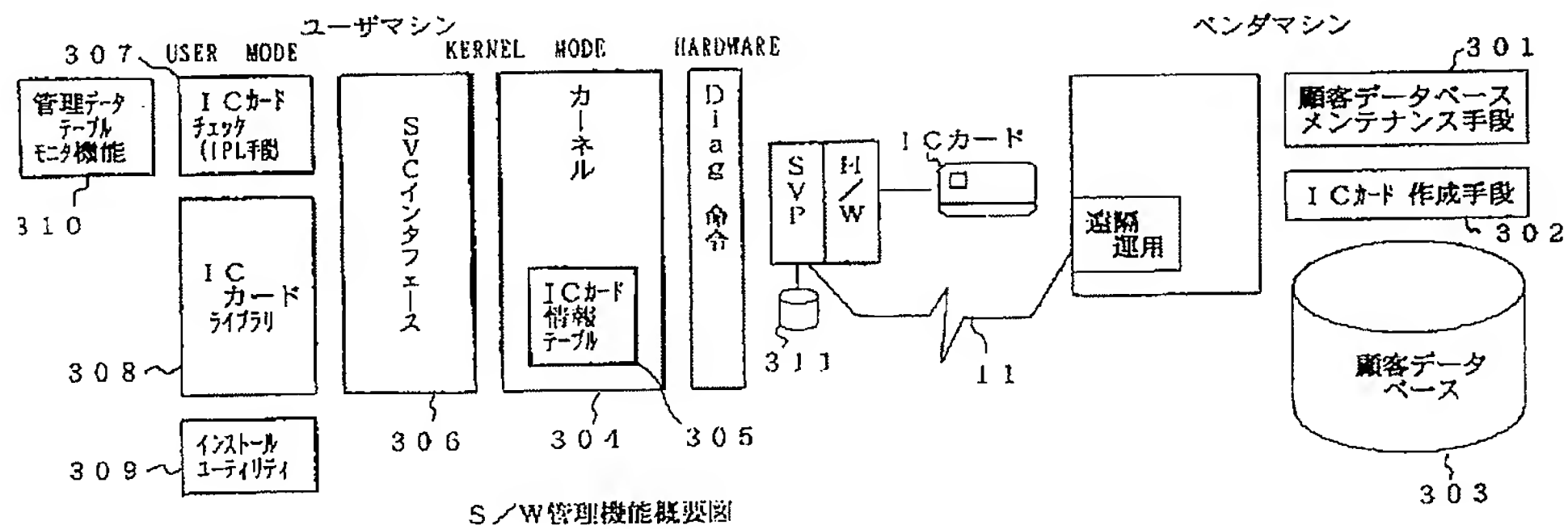
管理データテーブルの構成を示すブロック図

【図 8】



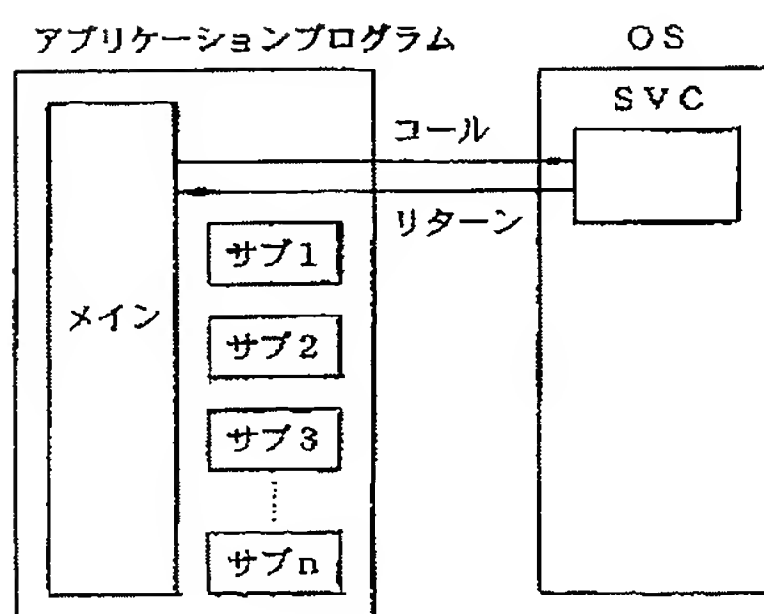
S/W管理機構のH/W構成図

【図 9】

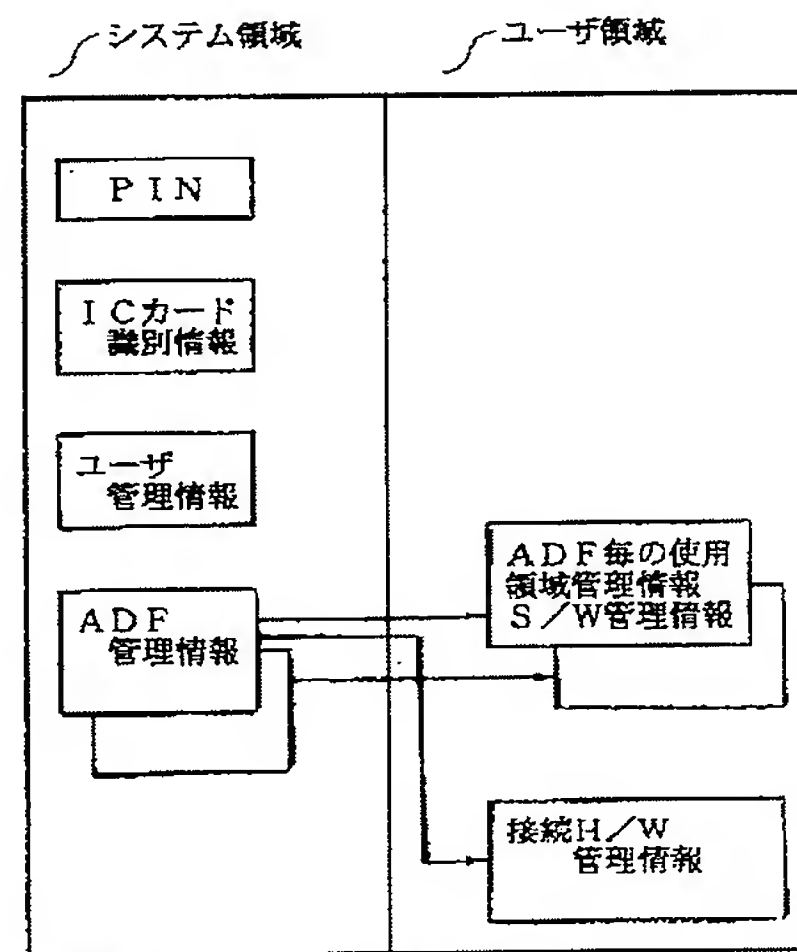


S/W管理機能概要図

【図 12】

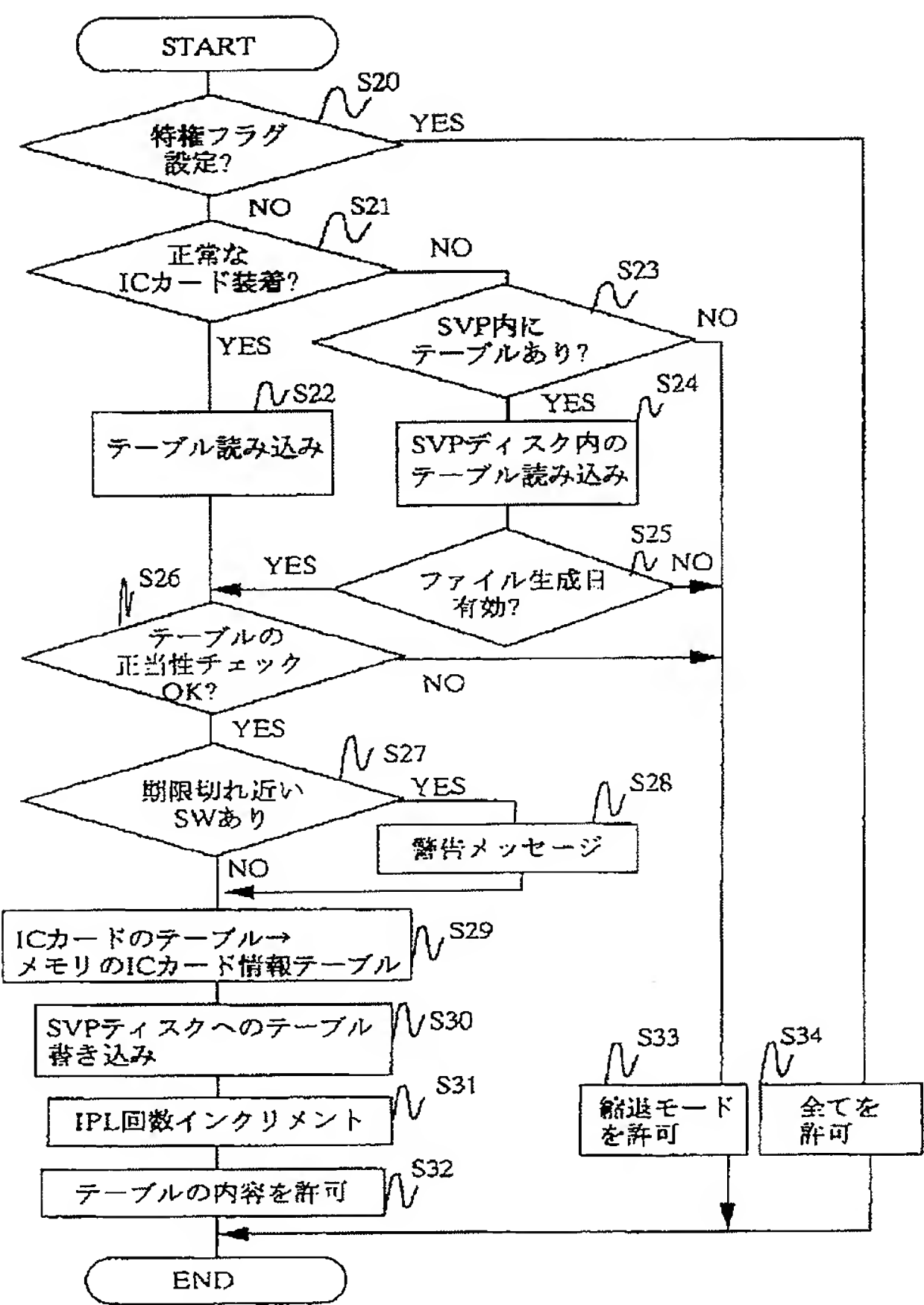


【図 15】



管理データテーブルの構成を示すブロック図

【図 1 1】



【図 1 7】

(a)

H/W-ID	H/Wのカテゴリ毎のID番号（被加付ノード識別子）
STARTDAY	H/Wのカテゴリ毎の登録日
LIMITDAY	H/Wのカテゴリ毎の使用有効期限
LIMITINFO	使用可能メモリアドレス範囲情報

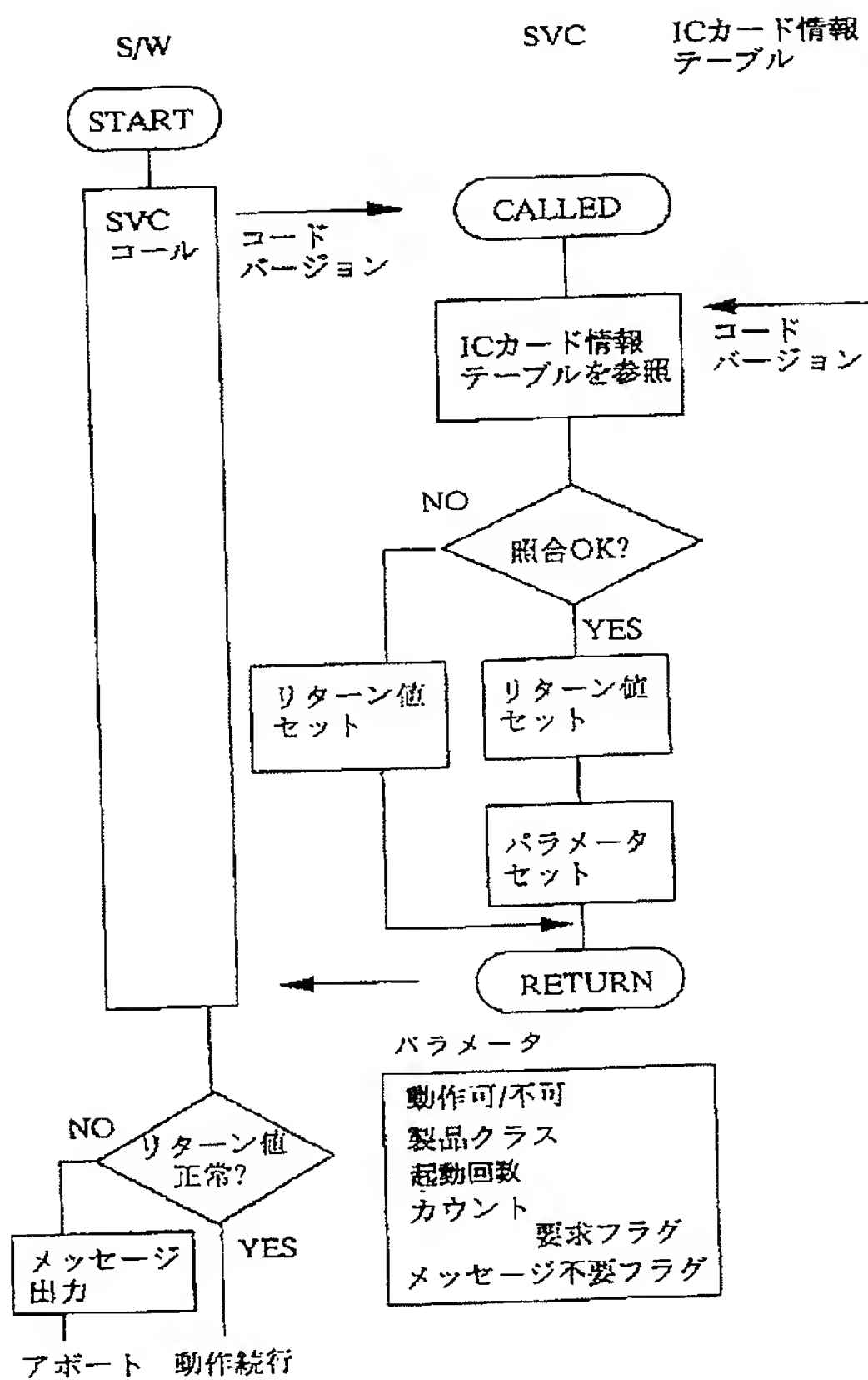
(b)

H/W-ID	H/Wのカテゴリ毎のID番号（被加付ノード識別子）
STARTDAY	H/Wのカテゴリ毎の登録日
LIMITDAY	H/Wのカテゴリ毎の使用有効期限
LIMITINFO	キャッシュメモリ割当アドレス範囲情報

(c)

H/W-ID	H/Wのカテゴリ毎のID番号（被加付ノード識別子）
STARTDAY	H/Wのカテゴリ毎の登録日
LIMITDAY	H/Wのカテゴリ毎の使用有効期限
LIMITINFO	使用可能クロック周波数情報

【図 1 3】



【図 1 8】

H/W-ID	H/Wのカテゴリ毎のID番号（被加付ノード識別子）
STARTDAY	H/Wのカテゴリ毎の登録日
LIMITDAY	H/Wのカテゴリ毎の使用有効期限
MODELCODE 1	モデルコード
LIMITNUM 1	最大接続台数（上記モデルコードのみを対象）
MODELCODE 2	モデルコード
LIMITNUM 2	最大接続台数（上記モデルコードのみを対象）
⋮	
MODELCODE n	モデルコード
LIMITNUM n	最大接続台数（上記モデルコードのみを対象）

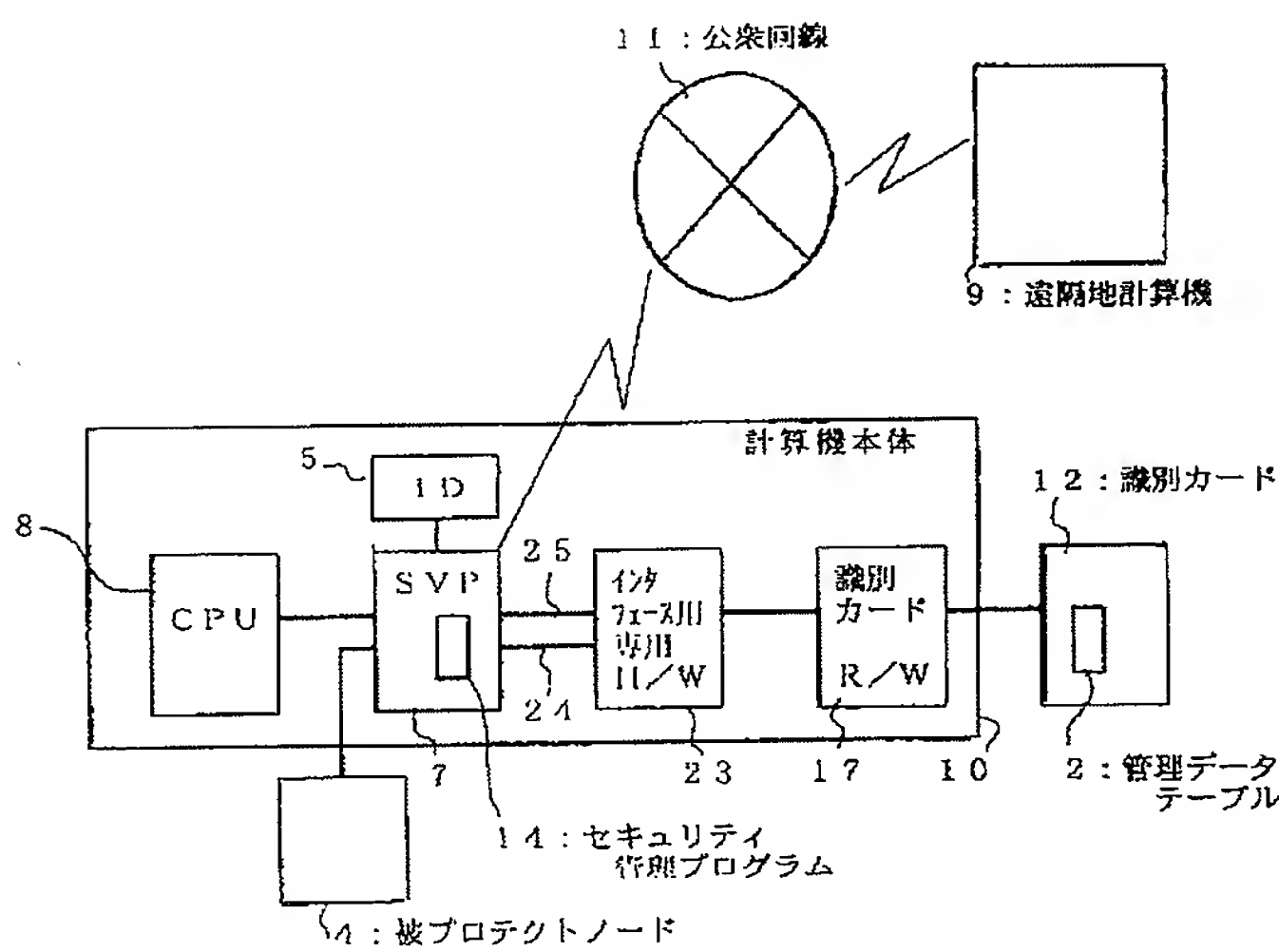
【図14】

ユーザ管理情報		100
名称	説明	
30 ディーラID	ディーラ識別ID	
31 ユーザID	ユーザ識別ID	
32 マシンID	機種/モデル識別ID	
33 ユーザレベル	システム使用者識別レベル	
34 使用開始可能日	ICカードの使用開始可能日	
35 有効期限	ICカードの使用有効期限	
36 更新日	ICカード内データの最終更新日	
37 ディーラ名	ユーザレベルに対応するディーラ名	
38 ユーザ名	システム使用者名	
39 マシン名	機種/モデル名	
40 CPU ID	CPU ID	
41 OS名	OS名	
42 OSバージョン名	OSバージョン名	
43 ワークステーション台数	OSのサポートワークステーション台数	
44 接続FXD台数	OSのサポートFXD台数	
45 主記憶装置容量	OSのサポート主記憶装置容量	
46 接続データベース台数	OSのサポートデータベースプロセッサ台数	
47 接続MT台数	OSのサポートMT台数	
48 計算機クロック周波数	その計算機で使用するクロック周波数	
49 キャッシュメモリ設定情報	キャッシュメモリとして設定するメモリ容量	
50 IPL回数	IPL回数	
ワークステーションモデルコード		
FXDモデルコード		
データベースプロセッサモデルコード		
MTモデルコード		

【図19】

H/W-ID	H/Wのカテゴリ毎のID番号(被プロテクト識別子)
STARTDAY	H/Wのカテゴリ毎の登録日
LIMITDAY	H/Wのカテゴリ毎の使用有効期限
ID 1	H/W1台毎に固有な識別子
ID 2	H/W1台毎に固有な識別子
⋮	
ID n	H/W1台毎に固有な識別子
LIMITNUM	最大接続台数

【図20】



(19)日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11)特許出願公表番号
特表2002-518720
(P2002-518720A)

(43)公表日 平成14年6月25日(2002.6.25)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 D 5 B 0 8 5

審査請求 未請求 予備審査請求 有 (全 66 頁)

(21)出願番号 特願2000-554109(P2000-554109)
(86) (22)出願日 平成11年6月9日(1999.6.9)
(85)翻訳文提出日 平成12年12月12日(2000.12.12)
(86)国際出願番号 P C T / U S 9 9 / 1 2 9 1 3
(87)国際公開番号 W O 9 9 / 6 5 2 0 7
(87)国際公開日 平成11年12月16日(1999.12.16)
(31)優先権主張番号 0 9 / 0 9 6 , 6 7 6
(32)優先日 平成10年6月12日(1998.6.12)
(33)優先権主張国 米国 (U S)
(81)指定国 E P (A T , B E , C H , C Y ,
D E , D K , E S , F I , F R , G B , G R , I E , I
T , L U , M C , N L , P T , S E) , J P

(71)出願人 マイクロソフト コーポレイション
MICROSOFT CORPORATI
ON
アメリカ合衆国 ワシントン州 98052-
6399 レッドモンド ワン マイクロソフ
ト ウェイ (番地なし)
(72)発明者 マリオ シー. ゴートゼル
アメリカ合衆国 98033 ワシントン州
カークランド ノースイースト 107 ブ
レイス 12631
(74)代理人 弁理士 谷 義一 (外2名)

最終頁に続く

(54)【発明の名称】 セキュリティ・ロケーション識別の方法およびシステム

(57)【要約】

ネットワーク・リソースへのアクセスが接続しているユーザのロケーションを含む情報に基づいている改善されたコンピュータ・ネットワーク・セキュリティ・システムおよび方法である。一般に、ユーザのロケーションの信頼性が低い場合、そのユーザに割り当てられるアクセス権はより制限される。識別機構およびプロセスは、ローカル・ユーザ、イントラネット・ユーザおよびダイアルアップ・ユーザなどを互いに区別するなど、セキュリティ方針のカテゴリに関してユーザのロケーションを決定する。ロケーションおよびユーザの資格認定を含む情報に基づいて、ユーザの通常のアクセス・トークン内のユーザに基づいたセキュリティ情報を越えてユーザのプロセスを制限せず、一方、ダイアルアップ接続を介して接続しているときには同じユーザのリソースへのアクセスをさらに制限するなどの、セキュリティ方針に従って、ユーザの通常のアクセスを制限できるアクセス・トークンが設定される。制限付きトークンは、好ましくは、信頼性がより低いロケーションから接続しているユーザのセキュリティ・コンテ

キストを制限することによる前記ロケーションに基づいた識別を実装するために使用される。

【特許請求の範囲】

【請求項1】 ユーザーが複数の仮想的なロケーションのうち1つのロケーションからネットワークに選択的に接続することができるコンピュータ・ネットワークにおいて、改善されたネットワーク・セキュリティを提供する方法であって、

前記ユーザーが接続しているロケーションを決定するステップと、

前記仮想的なロケーションを含む基準に基づいて少なくとも2つの異なるアクセス・レベルから前記ユーザーのアクセス・レベルを選択するステップと、

前記ユーザーを前記ネットワークに接続するステップと、

前記アクセス・レベルを含む情報に基づいて、ネットワーク・リソースへの前記ユーザーのアクセスを決定するステップ

とを備えることを特徴とする方法。

【請求項2】 前記ユーザーにインターネット・プロトコル・アドレスを割り当てるステップであって、前記割り当てられるアドレスはユーザーが接続しているロケーションによって決めるステップをさらに備えることを特徴とする請求項1に記載の方法。

【請求項3】 前記ユーザーが接続しているロケーションを決定するステップは、前記ユーザーに割り当てられたインターネット・プロトコル・アドレスを査定するステップを備えることを特徴とする請求項1に記載の方法。

【請求項4】 前記少なくとも2つの異なるアクセス・レベルからアクセス・レベルを選択するステップは、前記インターネット・プロトコル・アドレスに従って前記アクセス・レベルを選択するステップを備えることを特徴とする請求項3に記載の方法。

【請求項5】 前記ユーザーが接続しているロケーションを決定するステップは、前記ユーザーがリモート・アクセス・サーバを介して前記ネットワークに接続していることを決定するステップを備えることを特徴とする請求項1に記載の方法。

【請求項6】 前記ユーザーがダイヤルアップ接続を介して接続しているかどうかを決定するステップをさらに備えることを特徴とする請求項5に記載の方

法。

【請求項7】 前記ユーザーがダイヤルアップ接続を介して接続していると決定され、さらに、前記ユーザーが接続している電話番号を決定するステップと、前記電話番号を登録済みユーザーのリストと比較するステップとを含み、前記アクセス・レベルを選択するステップは、前記電話番号が前記リスト内にある場合には1つのレベルを選択し、前記番号が前記リストにない場合には別のレベルを選択するステップを備えることを特徴とする請求項6に記載の方法。

【請求項8】 前記ユーザーが接続しているロケーションを決定するステップは、前記ユーザーがリモート・アクセス・サーバを介して前記ネットワークに接続しているかどうかを決定するステップを備え、前記ユーザーがリモート・アクセス・サーバを介して接続している場合に、前記アクセス・レベルを選択するステップが、より多くの制限付きアクセス権に対応するアクセス・レベルを選択するステップを備えることを特徴とする請求項1に記載の方法。

【請求項9】 前記ユーザーが接続しているロケーションを決定するステップは、前記ユーザーがイントラネットを介して前記ネットワークに接続していることを決定するステップを備えることを特徴とする請求項1に記載の方法。

【請求項10】 前記ユーザーが接続しているロケーションを決定するステップは、前記ユーザーが仮想的な組織内ネットワークを介して前記ネットワークに接続していることを決定するステップを備えることを特徴とする請求項1に記載の方法。

【請求項11】 情報に基づいてネットワーク・リソースへのアクセスを決定するステップは、前記ユーザーの資格認定に基づいてアクセスを決定するステップを含むことを特徴とする請求項1に記載の方法。

【請求項12】 ネットワーク・リソースへのアクセスを決定するステップは、前記ユーザー用のアクセス・トークンを作成するステップを含むことを特徴とする請求項11に記載の方法。

【請求項13】 前記アクセス・トークンが前記ユーザーの各プロセスと関連付けられ、前記ネットワーク・リソースへのアクセスを決定するステップは、前記アクセス・トークン内の情報を各ネットワーク・リソースに関連付けられた

セキュリティ情報と比較するステップを含むことを特徴とする請求項12に記載の方法。

【請求項14】 前記アクセス・トークンを作成するステップは、前記ユーザーの通常のトークンから制限付きトークンを作成するステップと、前記制限付きトークンから前記親トークンに関連する少なくとも1つの特権を削除するステップとを含むことを特徴とする請求項12に記載の方法。

【請求項15】 アクセス・トークンを作成するステップは、前記ユーザーの通常のトークンから制限付きトークンを作成するステップと、前記通常のトークン内の対応するセキュリティ識別子の属性情報に関連した、前記制限付きトークン内のセキュリティ識別子の属性情報を、そのセキュリティ識別子を介したアクセスのみを拒否するために使用するように変更するステップとを含むことを特徴とする請求項12に記載の方法。

【請求項16】 前記ネットワークへ前記ユーザーを接続するステップは、前記ユーザーを、質疑応答型プロトコルを介して認証するステップを含むことを特徴とする請求項12に記載の方法。

【請求項17】 前記ユーザーを前記ネットワークへ接続するステップが、チケット発行機能によって発行されたチケットを前記ユーザーから受け取るステップを含むことを特徴とする請求項12に記載の方法。

【請求項18】 前記ユーザーを前記ネットワークへ接続するステップが、認証機関によって発行された前記証明を前記ユーザーから受け取るステップを含むことを特徴とする請求項12に記載の方法。

【請求項19】 アクセス・トークンを作成するステップは、前記ユーザーの通常のトークンから制限付きトークンを作成するステップと、少なくとも1つの制限付きセキュリティ識別子を前記制限付きトークンに追加するステップとを含むことを特徴とする請求項12に記載の方法。

【請求項20】 ネットワーク・リソースへのアクセスを決定するステップは、前記アクセス・トークン内のユーザー情報および少なくとも1つの制限付きセキュリティ識別子を、各ネットワーク・リソースに関連付けられたセキュリティ情報と比較するステップを含むことを特徴とする請求項12に記載の方法。

【請求項21】 ユーザーが複数の仮想的なロケーションのうち1つからネットワークへ選択的に接続することができるコンピュータ・ネットワークにおいて、改善されたネットワーク・セキュリティを提供するためのシステムであって、

ユーザーが接続する仮想的なロケーションを決定し、それに基づいて少なくとも2つの異なるアクセス・レベルから1つのアクセス・レベルを選択する識別機構と、

前記アクセス・レベルを含む情報に基づいて前記ユーザーのアクセス権を設定するセキュリティ・プロバイダと、

前記設定されたアクセス権に従ってネットワーク・リソースへのユーザー・アクセスを決定する実施機構

とを備えることを特徴とするシステム。

【請求項22】 前記識別機構は、それによって決定された前記仮想的なロケーションに基づいて前記ユーザーにインターネット・プロトコル・アドレスを割り当てることを特徴とする請求項21に記載のシステム。

【請求項23】 前記識別機構は、前記ユーザーに割り当てられたインターネット・プロトコル・アドレスを査定することを特徴とする請求項21に記載のシステム。

【請求項24】 前記識別機構は、前記インターネット・プロトコル・アドレスに従って前記アクセス・レベルを選択することを特徴とする請求項23に記載のシステム。

【請求項25】 前記識別機構は、前記ユーザーがリモート・アクセス・サーバを介して前記ネットワークに接続していることを決定することを特徴とする請求項21に記載のシステム。

【請求項26】 前記識別機構は、さらに、前記ユーザーがダイヤルアップ接続を介して接続していることを決定することを特徴とする請求項25に記載のシステム。

【請求項27】 登録済み電話番号のリストおよび前記識別機構に接続された発呼者ID機構をさらに備え、前記識別機構は発呼者ID機構にアクセスして

前記ユーザーの電話番号を決定し、前記リストにアクセスして前記電話番号が前記リスト内にあるかどうかを決定し、前記電話番号が前記リスト内にある場合は1つのアクセス・レベルを決定し、前記番号が前記リスト内にない場合に別のアクセス・レベルを決定することを特徴とする請求項26に記載のシステム。

【請求項28】 前記識別機構は、前記ユーザーがリモート・アクセス・サーバを介して前記ネットワークに接続しているかどうかを決定し、前記ユーザーがリモート・アクセス・サーバを介して接続している場合、さらに、前記ネットワークへの直接接続に対して選択される前記ユーザーのアクセス権に比較してより制限されたアクセス権に相当するアクセス・レベルを前記ユーザーに対して選択することを特徴とする請求項21に記載のシステム。

【請求項29】 前記識別機構は、前記ユーザーがイントラネットを介して前記ネットワークに接続している時日を決定するための手段を含むことを特徴とする請求項21に記載のシステム。

【請求項30】 前記識別機構は、前記ユーザーが仮想的な組織内ネットワークを介して前記ネットワークに接続している時を決定するための手段を含むことを特徴とする請求項21に記載のシステム。

【請求項31】 前記セキュリティ・プロバイダは、前記ユーザーの前記資格認定を含む情報に基づいて前記ユーザーのアクセス権を設定することを特徴とする請求項21に記載のシステム。

【請求項32】 前記セキュリティ・プロバイダは前記ユーザー用のアクセス・トークンを作成することを特徴とする請求項21に記載のシステム。

【請求項33】 前記アクセス・トークンは、前記ユーザーの各プロセスに関連付けられ、前記実施機構が前記アクセス・トークン内の情報を各ネットワーク・リソースに関連付けられたセキュリティ情報と比較することによって、前記ネットワーク・リソースへのアクセスを決定することを特徴とする請求項32に記載のシステム。

【請求項34】 ファイルをその上に有するコンピュータ・サーバ内において、前記ファイルへのアクセスを選択的に制限する方法であって、

要求をエンティティから受け取ってファイルへアクセスするステップと、

前記エンティティのタイプを含む基準に基づいて少なくとも2つの異なるアクセス・レベルから前記エンティティ用のアクセス・レベルを選択するステップと、

前記アクセス・レベルを含む情報に基づいて、前記エンティティの前記ファイルへのアクセスを決定するステップ

とを含むことを特徴とする方法。

【請求項35】 前記エンティティは、リモート・コンピュータ・システムのプロセスであって、前記少なくとも2つの異なるアクセス・レベルから前記エンティティ用のアクセス・レベルを選択する前記ステップは、前記ローカル・サーバのプロセスに対しては第1のアクセス・レベルを割り当て、前記リモート・コンピュータのプロセスに対しては第2のアクセス・レベルを割り当てるステップを含むことを特徴とする請求項34に記載の方法。

【請求項36】 前記エンティティは、前記コンピュータ・サーバ上で実行しているスクリプトであり、前記少なくとも2つの異なるアクセス・レベルから前記エンティティ用のアクセス・レベルを選択するステップは、スクリプトに対して異なるアクセス・レベルを割り当てるステップを含むことを特徴とする請求項34に記載の方法。

【請求項37】 前記エンティティは、前記コンピュータ・サーバ上で稼働しているFTPサーバであり、前記少なくとも2つの異なるアクセス・レベルから前記エンティティ用のアクセス・レベルを選択するステップは、FTPサーバに対して異なるアクセス・レベルを割り当てるステップを含むことを特徴とする請求項34に記載の方法。

【請求項38】 前記エンティティは、プロキシのプロセスであり、前記少なくとも2つの異なるアクセス・レベルから前記エンティティ用のアクセス・レベルを選択するステップは、前記ローカル・サーバのプロセス用に第1のアクセス・レベルを割り当て、プロキシのプロセス用に第2のアクセス・レベルを割り当てるステップを含むことを特徴とする請求項34に記載の方法。

【発明の詳細な説明】

【0001】

(発明の分野)

本発明は、一般にコンピュータ・システムに関し、より詳細には、コンピュータ・システムの改善されたセキュリティ・モデルに関する。

【0002】

(発明の背景)

現在のコンピュータ・セキュリティ・システムは、ユーザーの資格認定 (credentials) に従って与えられた許可に基づいて、ネットワーク・リソースへのユーザーのアクセスを決定する。このユーザー中心のモデルは、増大するモバイル／リモート (mobile/remote) ユーザー人口に大きな融通性を提供する。たとえば、リモート・アクセス・サーバおよびインターネットの接続性は、ユーザーが仮想的に任意のロケーションから会社のリソースにユーザーに意識させないで (transparently) アクセスすることを可能にする。

【0003】

この融通性はユーザーおよびネットワーク所有者（たとえば会社、企業）の両方に利点を提供するが、このような増大した有用性および簡単な接続性は本質的に、許可されないアクセスについてのリスクを引き上げる。暗号化されたネットワーク通信は有線盗聴を防ぐが、機密情報のある企業リソースへのリモート・アクセスを許すという本質的なリスクを依然として有している。実際には、リソース（ファイルなど）が送信されるときに保護されているにもかかわらず、正式に認可されたユーザーが適正な任意のロケーションからアクセスされることを会社が望まない企業リソースの機密情報を含むサブセットがある可能性が依然としてある。

【0004】

たとえば、ラップトップ・コンピュータのユーザーが飛行機の上で作業をしているときなどに、非常に機密性のある会社の戦略を意図しない閲覧者に不注意に表示する場合がある。新しい、広い視野角のラップトップ画面では、他の乗客がモニタの内容をのぞき見することを防ぐことはさらに困難である。同様に、モバ

イル・ユーザーの人口は増大しているので、ノートブック・コンピュータの盗難または紛失はさらに、機密性のある企業データのセキュリティを脅かしている。ユーザーのアカウントおよびパスワードも、特に盗まれたラップトップ上に維持されている場合は、盗まれる可能性がある。ユーザーが適切な資格認定を有する限り、既存のセキュリティ機構 (security mechanism) は、リモートからファイルをダウンロードし、他のリモート・アクションを実行することが容易とし、したがって、これらのセキュリティ・リスクおよび他のセキュリティ・リスクに寄与する。

【0005】

簡単に言えば、リモート・アクセス・サーバ (RAS) およびインターネットの接続性は、ユーザーが仮想的な任意のロケーションから企業リソースにアクセスできるようにする。しかし、一定のロケーション (特にリモート・ロケーション) は他よりも安全ではない。たとえば、軽便でアクセスが増大されているため、ラップトップ・コンピュータへダウンロードされたファイルは、会社のオフィス内にあるデスクトップ・マシン上のファイルより簡単に盗める。同様に、許可されない人がユーザーのアカウントおよびパスワードを得る可能性もあり、これによって、彼らがリモート・ロケーションから会社のリソースへアクセスしようとする可能性が最大になる。

【0006】

(発明の概要)

簡単に言えば、本発明は、ネットワーク・リソースへのアクセスが接続しているユーザーのロケーションを含む情報に基づいている改善されたコンピュータ・ネットワーク・セキュリティ・システムおよび方法を提供する。通常は、ユーザーのロケーションの信頼性がより低ければ、そのユーザーに割り当てられたアクセス権はより制限される。識別機構 (discrimination mechanism) は、ローカル・ユーザー、イントラネット・ユーザ、およびダイアルアップ・ユーザーを互いに区別するなど、いくつかのカテゴリのセキュリティ方針に関してユーザーのロケーションを決定する。セキュリティ・プロバイダは、ロケーションおよびユーザーの資格認定を含む情報に基づいて、そのユーザー用アクセス・トークンを設

定するなどによって、そのユーザーのアクセス権を確立する。実施機構(enforcement mechanism)は、そのユーザーのために設定されたアクセス権を使用して、リソースへのアクセスを許可または拒否するかどうかを決定する。ロケーションに基づいたアクセス権は、セキュリティ方針に従って、ユーザーの通常のアクセス権に関して制限することができる。たとえば、ローカル・ユーザーのプロセスは、ユーザーの通常のアクセス・トークン内のユーザーに基づいたセキュリティ情報を越えて制限することはできないが、一方、ダイアルアップ接続を介しての同じユーザーの接続は制限付きプロセスを有する場合がある。好ましい制限付きトークンを使用して、信頼性の低いロケーションから接続しているユーザーのアクセスを制限することによって、ロケーションに基づいた識別を実行する。制限付きトークンが使用され、信頼性の低いロケーションからのユーザー接続でのアクセスを制限するによるロケーション・ベースの識別を実行することは、望ましいことである。

【0007】

他の目的および利点は、図面を参照してなされる次の詳細な説明から明らかになるう。

【0008】

(詳細な説明)

例としての動作環境

図1および以下の考察は、本発明が実現できる適切なコンピューティング環境の簡単で一般的な説明を提供すること、を意図している。必要ではないが、本発明は、パーソナル・コンピュータによって実行されるプログラム・モジュールなどのコンピュータ実行可能な命令の一般的なコンテキスト内で説明される。一般に、プログラム・モジュールは、ルーチン、プログラム、オブジェクト、構成要素、データ構造、そして特定のタスクを実行するか、特定の抽象的なデータ・タイプに道具を提供するもの実現するなどを含む。さらに、当業者であれば、本発明は、ハンド・ヘルド・デバイス、マルチプロセッサ・システム、マイクロプロセッサ・ベースのプログラミング可能な消費者用電気製品、ネットワークPC、ミニ・コンピュータ、メインフレーム・コンピュータなどを含むほかのコンピュ

ータ・システム構成でも実行できることが理解されるであろう。本発明はまた、通信ネットワークを介してリンクされたりモート処理デバイスによってタスクが実行される分散コンピューティング環境内でも実行できる。分散コンピューティング環境では、プログラム・モジュールはローカル・メモリ記憶デバイスおよびリモート・メモリ記憶デバイスの両方に配置される場合がある。

【0009】

図1を参照すると、本発明を実現するための1例としてのシステムは、従来のパーソナル・コンピュータ20などの形の汎用コンピューティング・デバイスを含み、汎用コンピューティング・デバイスは、処理ユニット21、システム・メモリ22、および処理ユニット（processing unit）21のためのシステム・メモリを含む種々のシステム構成要素を結合するシステム・バス23を含む。システム・バス23は、メモリ・バスまたはメモリ・コントローラ、周辺バス、種々のバス・アーキテクチャのうち任意のアーキテクチャを使用するローカル・バスを含むいくつかのタイプのバス構成のどれでも含むことができる。システム・メモリは、読み取り専用メモリ（ROM）24およびランダム・アクセス・メモリ（RAM）25を含む。基本入出力システム26（BIOS）は、ROM24内に格納され、起動時などにパーソナル・コンピュータ20内の構成要素の間で情報を転送するのに役立つ基本的なルーチンを含んでいる。パーソナル・コンピュータ20はさらに、図示されてはいないがハードディスクから読み出したり書き込んだりするためのハードディスク・ドライブ27、取り外し可能な（removable）磁気ディスク29から読み出したり書き込んだりするための磁気ディスク・ドライブ28、および、CD-ROMまたは他の光媒体など、取り外し可能な光ディスク31から読み出したり書き込んだりするための光ディスク・ドライブ30を含む場合がある。ハードディスク・ドライブ27、磁気ディスク・ドライブ28、および光ディスク・ドライブ30はそれぞれ、ハードディスク・ドライブ・インタフェース32、磁気ディスク・ドライブ・インタフェース33、および光ドライブ・インターフェース34によってそれぞれシステム・バス23に接続されている。ドライブとその関連付けられたコンピュータ読み取り可能媒体は、パーソナル・コンピュータ20のためにコンピュータ読み取り可能命令、データ

構造、プログラム・モジュールおよびほかのデータの、不揮発性のストレージを提供する。ここに説明された例としての環境は、ハードディスク、取り外し可能磁気ディスク29および取り外し可能光ディスク31を使用しているが、当業者であれば磁気カセット、フラッシュメモリ・カード、デジタル・ビデオ・ディスク、ベルヌーイ・カートリッジ、ランダム・アクセス・メモリ(RAM)、読み取り専用メモリ(ROM)などの、コンピュータによってアクセス可能なデータを格納できる他のタイプのコンピュータ読み取り可能な媒体も例としての動作環境内で使用できることが理解されるであろう。

【0010】

オペレーティング・システム35（好ましくはWindows NT）、1つまたは複数のアプリケーション・プログラム36、ほかのプログラム・モジュール37およびプログラム・データ38を含むいくつかのプログラム・モジュールがハードディスク、磁気ディスク29、光ディスク31、ROM24またはRAM25に格納できる。ユーザーは、キーボード40およびポインティング・デバイス42などの入力デバイスを介してパーソナル・コンピュータ20にコマンドおよび情報を入力できる。他の入力デバイス（図示せず）は、マイクロフォン、ジョイスティック、ゲーム・パッド、サテライト・ディッシュ(satellite dish)、スキャナなどを含むことができる。これらおよび他の入力デバイスはしばしば、システム・バスに結合されたシリアルポート・インタフェース46を介して処理ユニット21に接続されているが、パラレル・ポート、ゲーム・ポートまたは汎用シリアルバス(USB)などの他のインターフェースによって接続されている場合もある。モニタ47または他のタイプの表示デバイスもまた、ビデオ・アダプタ48などのインターフェースを介してシステム・バス23に接続されている。モニタ47の外に、パーソナル・コンピュータは典型的にはスピーカおよびプリンタなどの他の周辺出力デバイス（図示せず）を含む。

【0011】

パーソナル・コンピュータ20は、リモート・コンピュータ49など1つまたは複数のリモート・コンピュータへの論理接続を使用してネットワーク化された環境内で動作する場合がある。リモート・コンピュータ49は、他のパーソナル

・コンピュータ、サーバ、ルータ、ネットワークPC、ピア・デバイス (peer device) または他の共通ネットワーク・ノードであり、典型的にはパーソナル・コンピュータに関連して上記に説明された要素の多くまたはすべてを含むことができるが、メモリ・ストレージ・デバイス50のみが図1に示されている。図1に描かれた論理接続は、ローカルエリア・ネットワーク (LAN) 51および広域ネットワーク (WAN) 52を含む。このようなネットワーク化環境はオフィス、全社的コンピュータ・ネットワーク、イントラネットおよびインターネットに普通に見られる。

【0012】

パーソナル・コンピュータ20はLANネットワーク化環境内で使用される際には、ネットワーク・インターフェースまたはアダプタ53を介してローカル・ネットワーク51に接続される。パーソナル・コンピュータ20はWANネットワーク化環境内で使用される際には、典型的にはモデム54または他の手段を含み、インターネットなど広域ネットワーク52上で通信を確立する。モデム54は内部あるいは外部に置かれる場合もあるが、シリアルポート・インタフェース46を介してシステム・バス23に接続されている。ネットワーク化された環境では、パーソナル・コンピュータ20またはその一部に関連して描かれたプログラム・モジュールは、リモートのメモリ・ストレージ・デバイス内に格納される場合がある。示されたネットワーク接続は例としてのものであって、コンピュータの間で通信リンクを確立する他の手段も使用できることが明らかであろう。

【0013】

ロケーション識別

本発明の一視点によれば、(ユーザーの資格認定に基づいたユーザーの通常のアクセス権の他に) ユーザーのロケーションに基づいてリソースへのアクセスを決定する方法およびシステムが提供される。たとえば、ローカルな安全なロケーションにいると決定された有効なユーザーには彼らの完全なアクセス権を与えられるが、一方、リモートのロケーションにいるユーザーは制限付きのアクセス権を与えられる。さらに、制限の量はリモート・アクセスのタイプに基づいて変化させることもできる。

【0014】

例として、図2はユーザーが（ローカル・マシン（複数可）を含む）企業ネットワーク60に接続することができる、多くのロケーションを示す。ユーザーは（図1に示されたようにLAN51およびネットワーク・インターフェース53など）ローカルエリア・ネットワークを介してコンピュータ62₁～62_nへ接続することができる。他のユーザーはたとえばT1接続を介してリモートのオフィス・サーバ64₁～64_nへ接続し、さらに他のユーザーは仮想的な組織内（VPN）66を介してインターネットを介して接続する場合がある。さらにべつのユーザーは、任意の数のリモート・アクセス・サーバ（たとえば68₁～68₂）を介して、他のロケーション（図示せず）から多くの方法で接続できる。

【0015】

本発明に遵守すれば、ネットワーク・リソースへアクセスするためにユーザーに許可されたアクセスのレベルは、所与のユーザーが接続した（仮想的な）ロケーションに依存する。たとえば、LAN62₁を介してローカル・マシン60に接続されたユーザーには完全なアクセス権を与えられるが、リモート・オフィス64₁を介したユーザーにはいくらか制限付きの権利、RAS68₁、68₂、またはVPN66を介したユーザーにはかなり制限付きのアクセス権を与えられる場合がある。

【0016】

ここに使用されているように、用語「ロケーション」は、接続がそこから発生しているという距離に関連する物理的な概念ではなく、接続ロケーションのタイプに関する論理的な概念であることが容易に分かるであろう。たとえば、ユーザーは任意のタイプの電話サービスを有する、仮想的な任意の物理的なロケーションからRAS68₂を介してネットワーク60に接続できる。同様に、ローカル・マシン60から比較的（物理的に）遠い可能性のある「イントラネット」のロケーションから接続する場合がある。実際に、RAS68₁、68₂ダイヤルアップ・ユーザーは、T1回線を介してリモート・オフィス64₁で接続しているユーザーよりも物理的な距離においては近い可能性があるが、ダイヤルアップ・ユーザーは通常は安全性が低いと考えられている。このように、ここに使用されて

いるようなロケーション、ユーザーが接続することのできる各ロケーションは、物理的なロケーションというより仮想的なロケーションと考えられる。それにもかかわらず、本発明はさらに、ユーザーの物理的なロケーションが実際に知られている場合には、物理的なロケーションに関連していくらかの動作をする場合もある（たとえば、本発明はさらに発呼者IDを介して、所定のエリア・コードから呼び出すすべてのRASユーザーへアクセスを制限する場合もある）。

【0017】

ロケーション識別を実行するために、ユーザーのロケーションを確実に決定するための機構／プロセス67が（たとえばネットワーク・マシン60内に）提供される。機構／プロセス67は、1つのマシン内に種々の構成要素を備える場合もあるし、ネットワーク内の種々の構成要素の間で分散される場合もある。さらに、ここに説明されたように、IPアドレスのロケーション識別に関しては2つの異なる機構がある。第1の機構はインターネット・ロケーション・サービス（ILS）69に基づいており、別の機構は種々のロケーションにいるクライアントに一定の範囲のIPアドレス（好ましくはディレクトリ・サービスによって管理されている）を割り当てること、そして信頼性のより低いロケーションから信頼性のより高いIPアドレスを使用することを防ぐために信頼できるルータを使用すること、に基づいている。どちらの方法もルーティング機構、および明確な信頼できるアクセスポイントを備えた任意のネットワーク上で機能する。

【0018】

ユーザーが信頼できるロケーションにいないかどうかを決定する第1の（ILS）方法は、機構67が、そのユーザーがリモート・アクセス・サーバ（RAS）を介して接続しているかどうかをチェックすることである。その際に、リモート・アクセス・サーバを介して接続しているのであれば、そのユーザーは、リモートで信頼性がより低い。この目的のために、図3のステップ300によって表されたように、RASがリモート・ユーザーのログオンを認証するとき、RASはユーザーにインターネット・プロトコル（IP）アドレスを割り当て、このユーザーおよびIPアドレスをILS（インターネット・ロケーション・サービス）69で登録する。図3の流れ図に示すように、IPアドレスがILSにリスト

されている場合（ステップ302）、ユーザーはこのRASクラスタを介してログオンしているので、信頼できない。このようなユーザーには、次に詳細に説明されるように、一定の削減されたアクセス・レベルを設定し（ステップ304）、次いでそのレベルを使用して（制限付きの）アクセス権を割り当てる（ステップ310）などによって、制限付きのアクセスを与えられる。

【0019】

しかし、ユーザーのIPアドレスがILS69内でRAS IPアドレスとしてリストされていない場合、そのユーザーは必ずしもローカルでもなく信頼もできない。例として、ユーザーがヨーロッパのRASサーバを介してログオンし、次いでそこを介してCharlotte（ノースカロライナ）ドメインへアクセスしたい場合、Charlotte RAS ILSはそのローカルILSにリストされたヨーロッパのRAS接続を有していない。したがって、ローカルILS69にリストされていないユーザーについては、ユーザーのロケーションを決定するために追加の情報が必要になる。

【0020】

追加情報の1つの断片は割り当てられたIPアドレスであり、これはステップ306で査定される。このIPアドレスが、ローカル・マシンによって割り当てられたローカルな、信頼できるIPアドレスの範囲内でない場合、ユーザーはローカルではない。したがって、ステップ306における機構／プロセス67はステップ304に分岐し、ここでは上記のようにレベルは信頼できないと設定される。しかしアドレスがローカルな信頼できるIPアドレスの範囲内にある場合、ユーザーはローカルではあってしかもRASを介して接続しておらず、したがって信頼できる。このようなユーザーには、以下に詳細に説明されるように、ユーザーに信頼できるアクセス・レベルを割り当て（ステップ308）、次いでそのレベルを使用してアクセス権を割り当てる（ステップ310）などによって、通常のアクセスを与えられる。

【0021】

接続のための完全なルーティング・パスはサーバに使用可能であり、したがってロケーションを決定するときに、アクセスは、ユーザーの packets がルーティ

ングされているもっとも信頼性の低いロケーション（すなわち「もっとも弱いリンク」）に基づいて割り当てられる。さらに、IPアドレスが「信頼できない」ロケーションの範囲内になく、信頼できる範囲内にあるとは仮定されず、ロケーション識別の性質は排他的ではなく包括的であり、すなわち、信頼できるIP範囲のリストは信頼できないロケーションのリストを脱落することによってレベルを割り当てるのではなく、レベルを割り当てることをテストされる。

【0022】

他の電子セキュリティ・システムと同様に、一般に、本発明が使用される配慮のレベルはまた、全体的なセキュリティの結果についても責任を有する。たとえば、ネットワークを異なる信頼レベルで分離するときに配慮が行われるべきであり、細目は適切にルーティングされるべきであり、内部の手続きはたとえば、だれかが個人的な使用のために会社のオフィス内のデスクトップ・マシン上にRASサーバをインストールできないようにすべき、などである。

【0023】

上記の例は簡単な、2つのレベルのローカルな識別機構67を提供する。しかし、多数の信頼レベル制御をより細かく細分化するために、IPアドレスは、ユーザーが接続しているロケーションに関する追加のロケーション情報に対応する範囲内でサーバによって割り当てられることもできる。RASサーバはさらにロケーション識別機構71で構成され、「許可された」電話番号からの発呼者に関しては1つの範囲で、無名のまたは登録されていない電話番号に関しては別の範囲で、IPアドレスを割り当てることもできる。機構／プロセス71は、上記の機構／プロセス67と同じまたは同様の構成要素および追加の構成要素を含み、1つのマシン内にある場合もあり、またはネットワーク内の多くのマシンの間で分散されている場合もあることに注意されたい。しかし、より細かい細分性を提供する他に、ドメイン・サーバにおいて信頼できるIPアドレス範囲を維持すると、照会時にILS69でチェックするより時間がかからない。さらに、次に明らかになるように、全体的なセキュリティを達成するには、ロケーションマッピングへのグローバルなアドレスのデータベース、信頼できるアドレス割り当ておよび安全なルータ／ゲートウェイを含む、3つの部分の機構が一般にあることが

明らかであろう。

【0024】

次の表は、架空の会社のために恣意的に設定された所定の方針に基づいて、ユーザーに割り当てられる可能性のある信頼レベルおよびIPアドレスを示したものである。ローカル・マシンへ直接（たとえばLANインターフェース・カード53を介して）接続しているユーザーはレベル0の信頼性である。

【0025】

【表1】

レベル	ロケーション	IPアドレスの範囲
信頼レベル1	ローカルな イントラネット・ユーザ	111.22.0.0-111.22.255.255 111.24.0.0-111.24.127.255
信頼レベル2	RAS許可ユーザー	111.24.128.255-111.24.255.255
信頼レベル3	RAS無名ユーザー	111.25.0.0-111.25.255.255

【0026】

例として、図4はユーザーがRASサーバ（たとえば、68₂）へ接続する際に経由するユーザー接続の、3つの異なる³⁰タイプを示す。第1のユーザーはRAS登録済み電話番号からダイヤルインすることによって、リモート・コンピュータ70₁をRASサーバ68₂へ接続し、第2のユーザーは未登録またはブロックされた電話番号を介してリモート・コンピュータ70₂から接続し、第3のユーザーは任意の電話番号から接続する。最初の2人のユーザーは自分がシステムの許可されたユーザーであることを主張するユーザー認証を有するが、第3のユーザーは許可されたユーザーであると主張⁴⁰せず、ゲストとして接続しようとしているのみである。アクセス・レベルを決定するために、RASサーバ68₂はまず、発呼者ID74を介して、呼び出し側コンピュータの電話番号を決定する。電話番号が使用可能な場合（たとえば発呼者によってブロック（妨害）されていない場合）、RASサーバ68₂は、データベース（またはテーブル）72に問い合わせる。このデータベースは、リソースへの拡大されたアクセスを許可されて

いる登録済み電話番号のリストを保持している。この方法で、登録済み番号から呼び出すリモート・コンピュータ70₁のユーザーに対して、未登録の電話番号またはブロックされた電話番号から呼び出すリモート・コンピュータ70₂のユーザーよりも、リソースへのより大きなアクセスを与えることが可能になる。さらに、70₁のユーザー、70₂のユーザーの双方は、ゲスト・ユーザ70₃の電話番号にかかわらず、ゲスト・ユーザ70₃よりも大きなアクセス権を有することが可能になる。たとえば、リモート・コンピュータ70₃のユーザーは公共サーバ76上のファイルへのアクセスのみを許可されるが、一方、未登録の番号から呼び出すユーザー・コンピュータ70₂は、公共サーバ76および従業員サーバ78へのアクセスを有する可能性がある。最後に、登録済み番号から呼び出すユーザー・コンピュータ70₁は、公共サーバ76、従業員サーバ78、および機密サーバ80にアクセスを有するが、トップ・シークレットサーバ82にはアクセスを有しない可能性がある。このような区別は、会社が任意の数のアクセス方針を設定することを可能にする。上記の例では、移動中の従業員は未登録のロケーションから呼び出して一部の従業員レベルのファイルにアクセスすることはできるが（さらに彼らのユーザー資格認定によって制限される）、しかし機密ファイルにはアクセスできないことになる。機密ファイルは、ユーザーの家または登録済み電話番号を有する他の知られたロケーションからのみアクセスでき、一方、トップ・シークレット・ファイルはどのRAS接続を介してもアクセスできない。

【0027】

まとめると、図5～6は、既定の方針に基づいてアクセス・レベルが割り当てられる方法を示す、例としての流れ図を含む。図5のステップ500でユーザーがローカル・マシン60を介して接続している場合、ステップ502で信頼レベルは0に設定され、これは次いでステップ516に続き、ここではアクセス権は信頼レベルに基づいて（部分的に）割り当てられる。しかし、ローカル・マシンを介して接続していない場合、プロセス／機構71は図6に続き、ここではリモート接続のタイプが割り当てられたIPアドレスを介して信頼レベルを決定する。図6のステップ520でユーザーがダイアルアップ接続を介して接続していな

い場合、ステップ520はステップ522へ分岐し、そのユーザーに割り当てられたIPアドレスは、ローカル・イントラネット・ユーザのために保存されたアドレスの範囲内である。この簡単な例では、ユーザーはローカル・マシンに直接接続するか、イントラネット接続を介するかまたはダイヤルアップ接続を介して接続するかのいずれかであることを注意されたい。

【0028】

しかし、ステップ520でユーザーがダイヤルアップ接続を介して接続していると検出された場合、ステップ520はステップ524に分岐し、接続が行われている電話番号を決定する。この情報は発呼者ID機構72などを介して使用可能にされる場合があることが理解されるであろう。呼び出し発生時にユーザーが発呼者ID機能をブロック（妨害）している可能性、または発呼側電話が機能を稼働できない（たとえば、発呼側電話が発呼者IDを備えた領域以外のロケーションにある場合など）可能性があるため、ステップ526はその電話番号が使用可能かどうかをテストし、決定する。機構72が、必要な場合には意図的にブロックされた呼び出しと、検出できないだけの呼び出しとを区別する機能がある場合、方針は2つのタイプを区別し、異なる信頼レベルを設定できることに注意されたい。しかし、この例では、どういう理由でも電話番号が使用可能でない場合、ステップ526はステップ532に分岐し、そこでIPアドレスは、RAS未登録ユーザー範囲内で割り当てられる。

【0029】

しかし、ステップ526でその番号が使用可能な場合、ステップ528が実行され、ここでは番号を使用してデータベース74などを問い合わせ、その番号が既定の信頼できるロケーションとして登録済み番号であるかどうかを決定する。この時点で、ロケーション情報はオプションとしてユーザー識別と組み合わせられる場合があり、たとえば、ユーザーXと識別されたユーザーは、彼または彼女の登録済みの家の番号から呼び出している場合には拡大されたアクセスを与えられるが、その他のユーザーはその番号から呼び出しても拡大されたアクセスを受け取らないことに注意されたい。

【0030】

ステップ530によって番号が適切に登録されていると決定された場合、ステップ530はステップ534に分岐し、ここでIPアドレスは発呼側コンピュータに関するRAS登録済みユーザー範囲内で割り当てられる。番号が適切に登録されていると決定されなかった場合、ステップ530はステップ532に分岐し、ここでIPアドレスはRAS未登録ユーザー範囲内で割り当てられる。ロケーション識別プロセス／機構71は次いで図5のステップ504に戻り、ここで割り当てられたアドレスはアクセス権を決定するマシンによって査定される。

【0031】

ステップ504でIPアドレスがローカル・イントラネット・ユーザの範囲内にある場合、ステップ504はステップ506に分岐し、ここでは信頼レベルはこのユーザーについて1と設定される。IPアドレスがローカル・イントラネット・ユーザの範囲内にない場合、ステップ508はその範囲がRAS登録済みユーザーの範囲内にあるかどうかをテストし決定する。範囲内にある場合、ステップ510で信頼レベルは2に設定されるが、範囲内にない場合、信頼レベルはステップ512で3と設定される。信頼レベルが0から3に一度設定されると、プロセスは次にステップ516に続き、次に詳細に説明するようにここでユーザーの資格認定の組み合わせにおけるユーザーの信頼レベルに基づいてアクセス権が割り当てられる。

【0032】

図7は一般に、本発明によるアクセス権を決定するための論理を示す。セキュリティ・プロバイダ88はユーザー資格認定90およびロケーション情報（たとえば信頼レベル）92をとり、その情報に基づいてそのユーザーのためのアクセス権94を決定する。次に説明するように好ましい実施形態では、アクセス権はユーザーのプロセスの各々に関連付けられたアクセス・トークン内におかれ、各リソースに関連付けられたセキュリティ情報と比較されて、そのリソースへのアクセスを決定する。

【0033】

制限付きトークンを使用したロケーションの識別

次に明らかになるように、本発明は好ましくはオペレーティング・システム・

レベルで実装され、したがって、実質的にアクセス情報に関してすべての可能性をカバーする。例として、サーバ上の所与のファイルを保護することを考えてみる。このファイルは、リモートSMBファイル・アクセス、サーバ上で実行しているスクリプトを介して、サーバ上で実行しているFTPサーバを介して、プロキシ（第3のマシン）を介してなど、多くの方法でアクセスできる。本発明はシステム・レベルで動作し、実質的にファイルにアクセスするすべての方法を保護することを可能にする。

【0034】

ここに説明された本発明の好ましいセキュリティ・モデルは、既存のWindows NTセキュリティ・モデルを強化し、拡張する。しかし、本発明をWindows NTオペレーティング・システムに限定する意図はなく、逆に、本発明は、何らかの方法で入力情報に基づいてリソースへのアクセスを限定できる任意の機構で動作し、利益を与えることが目的とされている。

【0035】

一般に、Windows NTオペレーティング・システムでは、ユーザーはプロセス（およびそのスレッド）を介してシステムのリソースにアクセスすることによってタスクを実行する。簡単に説明するために、プロセスおよびそのスレッドは概念上等価と見なされ、今後は簡単にプロセスと呼ぶ。また、Windows NT内ではオブジェクトによって表される、ファイル、共有メモリおよび物理デバイスを含むシステムのリソースは、本明細書では通常リソースまたはオブジェクトと呼ばれる。

【0036】

ユーザーがWindows NTオペレーティング・システムにログオンし認証されると、セキュリティ・コンテキストがそのユーザーのためにセットアップされ、この中にはアクセス・トークン100の構築も含まれる。図8の左側に示すように、従来のユーザー・ベースのアクセス・トークン100は、UserAndGroupsフィールド102を含む。UserAndGroupsフィールド102は、セキュリティ識別子、すなわち、ユーザーの証明およびそのユーザーが属するグループ（たとえば編成内のグループ）を識別する1つまたは複数

のグループID106に基づいたセキュリティ識別子（セキュリティIDまたはSID）104を含むトークン100はまた、そのユーザーに割り当てられた任意の特権を一覧する特権フィールド108を含む。たとえば、このような特権の1つは、管理レベルのユーザーに、特定のアプリケーション・プログラミング・インタフェース（API）を介してシステム・クロックを設定する能力を与える場合がある。特権は、アクセス制御チェック、これは次に説明されるが、特権がない場合はオブジェクトへのアクセスを許可する前に実行されるアクセス制御チェックに優先することに注意されたい。

【0037】

次に詳細に説明され、図9に一般に示されるように、オブジェクト112へのアクセスを所望するプロセス110は、所望するアクセスのタイプを指定し（たとえばファイル・オブジェクトへの読み取り／書き込みアクセスを得るなど）、および、カーネル・レベルでは関連付けられたトークン100をオブジェクト・マネジャー114に提供する。オブジェクト112はそれに関連付けられたカーネル・レベルのセキュリティ記述子116を有し、オブジェクト・マネジャー114はセキュリティ記述子116およびトークン100をセキュリティ機構118に提供する。セキュリティ記述子116の内容は、典型的にはオブジェクトの所有者（たとえば制作者）によって決定され、一般に（任意に）アクセス制御エントリーのアクセス制御リスト（ACL）120を含み、各エントリーについて、そのエントリーに対応する1つまたは複数のアクセス権（許可されたアクションまたは拒否されたアクション）を含む。各エントリーはタイプ（拒否または許可）インジケータ、フラグ、セキュリティ識別子（SID）およびアクセス権をビット・マスクの形で含み、各ビットは許可に対応する（たとえば、1つのビットは読み取りアクセス、1つのビットは書き込みアクセス、など）。セキュリティ機構118はトークン100内のセキュリティIDおよびプロセス110によって要求されたアクション（複数可）のタイプをACL120内のエントリーと比較する。許可されたユーザーまたはグループに関して一致が発見され、所望のアクセスのタイプがそのユーザーまたはグループに許可可能な場合、オブジェクト112へのハンドルはプロセス110に戻されるが、その他の場合は、アクセ

スは拒否される。

【0038】

例として、ユーザーを「会計」グループのメンバーとして識別するトークンを持つユーザーが読み取りおよび書き込みアクセスで特定のファイル・オブジェクトにアクセスしたいとする。ファイル・オブジェクトが、ACL120のエントリー内で許可されたタイプの「会計」グループ識別子を有し、そのグループが読み取りおよび書き込みアクセスを使用可能にする権利を有する場合、読み取りおよび書き込みアクセスを許可するハンドルは戻されるが、その他の場合は、アクセスは拒否される。効率上の理由から、セキュリティ・チェックはプロセス110がまずオブジェクト112（作成または開く）にアクセスしようと試みたときのみ実行され、したがってそのオブジェクトに対するハンドルはそれを介して実行できるアクションを制限するように、アクセス情報のタイプを格納することに注意されたい。

【0039】

セキュリティ識別子116はまた、システムACLまたはSACL121を含み、これは監査されるべきクライアント・アクションに対応するタイプ監査のエントリーを含む。各エントリー内のフラグは監査が成功したオペレーションまたは失敗したオペレーションのどちらを監視するかを示し、エントリー内のビット・マスクは監査されるべき動作のタイプを示す。エントリー内のセキュリティIDは、監査されているユーザーまたはグループを示す。たとえば、ファイル・オブジェクトへの書き込みアクセスを有しないグループのメンバーがそのファイルに書き込もうと試みた場合いつでも決定できるように特定のグループが監査されている状況を考える。そのファイル・オブジェクトに関するSACL121は、その中にグループ・セキュリティ識別子と、適切に設定された失敗フラグおよび書き込みアクセス・ビットを有する監査エントリーを含む。その特定のグループに属するクライアントがそのファイル・オブジェクトに書き込みしようとして失敗するといつでも、そのオペレーションは記録される。

【0040】

ACL120は、（すべての権利または選択された権利に関して）グループ・

ユーザーにアクセスを許可するのではなく、アクセスを拒否するためにマークされる1つまたは複数の識別子を含む場合があることに注意されたい。たとえば、ACL 120内にリストされた1つのエントリーは、その他の場合には「グループ₃」のメンバーにオブジェクト112へのアクセスを許可するが、ACL 120内の他のエントリーは特に、「グループ₂₄」のすべてのアクセスを拒否する場合がある。トークン100が「グループ₂₄」セキュリティIDを含んでいる場合、アクセスは「グループ₃」のセキュリティIDの存在にかかわらず拒否されることになる。もちろん、セキュリティ・チェックは正しく機能するために、「グループ₃」エントリーを介したアクセスを許可しないようにアレンジされ、その後、すべてのDENY（拒否）エントリーをACL 120の前面に置くなどによって、グループ₂₄エントリーの「DENY ALL（すべて拒否）」状態をチェックする。この構成（arrangement）は、グループの残りのメンバーの各々を個別にリストしてそのアクセスを許可する必要なく、グループの、1人または複数の分離したメンバーが個別にACL 120内で排除できるので、向上した効率を提供することが明らかであろう。

【0041】

アクセスのタイプを指定する代わりに、発呼者はMAXIMUM_ALLOWEDアクセスを要求することもでき、これによって、アルゴリズムは通常のUser And Groups リスト対ACL 120内の各々のエントリーに基づいて、許可される最大のアクセス・タイプを決定することに注意されたい。より詳しくは、アルゴリズムは所与のユーザーのための権利を蓄積してい識別子のリストをウォーク・ダウン（すなわち、種々のビット・マスクをORする）。権利が一度蓄積されると、ユーザーに蓄積された権利が与えられる。しかし、ウォーク・スルーの間にユーザー識別子またはグループ識別子および要求された権利に一致する拒否エントリーが発見されると、アクセスは拒否される。

【0042】

制限付きトークンは（制限付きまたは制限なしのいずれかの）既存のアクセス・トークンから作成され、ユーザーの通常のトークンよりも少ないアクセスを有する（すなわち、その権利および特権のサブセットを有する）。ここに使用され

ているように、ユーザーの「通常の」トークンは、（ユーザーまたはグループを介する）ユーザーの識別に基づいてのみアクセスを許可し、他には追加の制限がないトークンである。制限付きトークンは、ユーザーの通常のトークンがこれらのS I Dを介してアクセスを許可している場合でも、特に「USE__FOR__DENY__ONLY」とマークされた1つまたは複数のユーザーまたはグループのセキュリティ I Dを介したリソースへのアクセスを許可されず、および／または、ユーザーの通常のトークン内にある特権を削除する場合がある。また次に説明するように、制限付きトークンが任意の制限付きセキュリティ I Dを有する場合、トークンは追加のアクセス・チェックを受け、ここで制限付きセキュリティ I DはオブジェクトのA C L内のエントリーと比較される。

【0043】

本発明の一態様によれば、アクセス・トークンはユーザーの識別およびユーザーが接続しているロケーションの両方に基づいて、そのユーザーのために作成される。一般に、そのロケーションの信頼性が低いと、関連付けられたプロセスがアクセスできるリソースに関して、および／または、そのトークンがこれらのリソースについて実行できるアクションに関して、そのトークンはより制限を受ける。たとえば、L A Nを介して接続しているユーザーはそのユーザーのプロセスに関連付けられた通常のトークンを有する可能性があるが、一方、R A Sを介して接続された同じユーザーでは、彼または彼女のプロセスはすべての特権をはぎ取られた制限付きトークンに関連付けられる可能性がある。

【0044】

上記のように、アクセスを削減する1つの方法は、制限付きトークンの中で1つまたは複数のユーザーおよび／またはグループのセキュリティ識別子の属性を変更して、アクセスを許可するのではなくアクセスを許可できないようにすることである。USE__FOR__DENY__ONLYとマークされたセキュリティ I Dは、アクセスを許可する目的のためには効果的に無視されるが、そのセキュリティ I Dに関して「DENY（拒否）」エントリーを有するA C Lは、依然としてアクセスが拒否される。例として、制限付きトークン124（図9）内のグループ₂のセキュリティ I DがUSE__FOR__DENY__ONLYとマークされ

ている場合、ユーザーのプロセスが、グループ₂を許可されたものとしてリストしているACL 120を有するオブジェクト112へアクセスしようと試みたとき、このエントリーは効果的に無視され、プロセスは他の何らかのセキュリティIDによってアクセスを得なければならないことになる。しかし、ACL 80が要求されたタイプのアクションに関してグループ₂をDENYとしてリストしているエントリーを含んでいる場合、一度テストされると、他のセキュリティIDにかかわらずアクセスは許可されない。

【0045】

これはサーバに、ユーザーまたはグループがユーザーのロケーションに基づいてオブジェクトへアクセスすることを制限する能力を与えることが理解されるであろう。上記のように、IPアドレス範囲はユーザーのロケーションに基づいて、たとえば、ローカル・マシンへ接続している場合は信頼レベル0、イントラネットまたは他の信頼できるロケーションから接続している場合は信頼レベル1、許可された電話番号からRASを介している場合はレベル2、その他の場合はレベル3と指定できる。このアドレスの範囲は次いで検査され、所定のグループをUSE__FOR__DENY__ONLYとマークする。

【0046】

例として、それぞれ、（それらのACLに基づいて）トップ・シークレット・ファイル、機密ファイル、従業員ファイルへアクセスを許可する、「トップ・シークレット」SID、「機密」SID、および「従業員」SIDを含む通常のアクセス・トークンを有するユーザーXとして識別されたユーザーを考えてみる。ユーザーXが信頼レベル0であった場合、ユーザーXの通常のトークンが使用され、そこにはロケーションに基づいた制限はない。しかし、信頼レベル1では、トップ・シークレットSIDは、ユーザーXのアクセス・トークンの中でUSE__FOR__DENY__ONLYとマークされる。同様に、信頼レベル2では、トップ・シークレットSIDおよび機密SIDの両方がUSE__FOR__DENY__ONLYとマークされ、一方、レベル3では、トップ・シークレットSID、機密SIDおよび従業員SIDがUSE__FOR__DENY__ONLYとマークされる。セキュリティIDは一部のオブジェクトのACL内では「DENY」と

してマークされ、その識別子を削除すると、これらのオブジェクトへのアクセスを拒否するのではなく許可することになるため、セキュリティIDをユーザーのトークンから削除するだけでは、オブジェクトへのアクセスを安全に削減できないことに注意されたい。さらに、このUSE_FOR_DENY_ONLYセキュリティ・チェックをオフにする機構は提供されていない。

【0047】

制限付きトークン内でアクセスを削減する別の方法は、親トークンに関連する1つまたは複数の特権を削除することである。たとえば、管理特権を伴う通常のトークンを有するユーザーは、ユーザーがローカル・マシン60に直接接続されていない限り、ユーザーのプロセスがまったく特権を有しないか、何らかの方法で削減された特権を有する制限付きトークンで実行するように、本発明のロケーションに基づいたシステムを介して制限することができる。残る特権はまた、たとえば、ローカル（レベル0）の場合はすべての特権、レベル1の場合は一部の特権、レベル2または3の場合はまったく特権なしなど、信頼のレベルに基づいている場合があることが理解されるであろう。

【0048】

ユーザーのロケーションに基づいてトークンのアクセスを削減するさらに別の方法は、そこに制限付きセキュリティIDを追加することである。制限付きセキュリティIDは、プロセス、リソース動作などを表す番号であり、GUIDに接頭部または、暗号ハッシュなどを介して生成された番号を追加するなどによってユニークになっており、これらのセキュリティIDを他のセキュリティIDから区別するための情報を含むことができる。以下に説明するように、トークンが制限付きのセキュリティIDを含む場合、そのトークンは追加のアクセス・チェックを受け、ここで制限付きセキュリティIDはオブジェクトのACL内のエントリーに対して比較される。したがって、たとえば制限付きSIDは「RAS」を指定し、これによって、オブジェクトのACLが「RAS」エントリーを有しないかぎり、ユーザーはそのオブジェクトへのアクセスを拒否されることになる。

【0049】

図9に示されたように、制限付きセキュリティIDは制限付きトークン124

の特別なフィールド122に置かれ、本発明によって、プロセスがアクションを要求するロケーションを識別することができる。以下に詳細に説明されるように、少なくとも1つのユーザー（またはグループ）セキュリティIDおよび少なくとも1つの制限付きセキュリティIDがそのオブジェクトへのアクセスを許可されるように要求することによって、オブジェクトはそのロケーション（同時にユーザーまたはグループ）に基づいて選択的にアクセスを許可できる。さらに、ロケーションの各々は異なるアクセス権を許可される場合もある。

【0050】

この設計は、ユーザーが所与のロケーションから実行を許可されていることを制御するため、ユーザーのコンテキストに重要な融通性および細分性を与える。例として、ローカル・マシンに接続しているユーザーはレベル0の信頼性、イントラネットおよび信頼できるロケーションから接続しているユーザーはレベル1の信頼性、（RASを通じて）許可された電話番号およびインターネットから接続しているユーザーはレベル2の信頼性、および制限付きのロケーションまたは許可されていない電話番号から接続しているユーザーはレベル3の信頼性である、上記の例を考えてみる。すると、ユーザーのロケーションに基づいて（たとえば、ユーザーのIPアドレスから確かめられたように）、レベル0からレベル3の信頼性を、次のように実行される何らかの既定の方針に基づいて定義することができる。

【0051】

【表2】

レベル	セキュリティ・コンテキスト内での制限
0	ユーザーのセキュリティ・コンテキストに追加の制限はない
1	ユーザーは、たとえば、バックアップ／復元など非常に微妙な動作から除去された特権を有するなど、制限付きコンテキストの基でオペレーションを実行する。
2	ユーザーは、すべてのSIDが依然として実行可能だが、特権を有しない制限付きコンテキストの元でオペレーションを実行する。
3	ユーザーは、制限付きコンテキストの元で操作し、制限付きコンテキストは、たとえば、全員および認証されたユーザーなど一定の人をのぞいて、USE_FOR_DENY_ONLYビットを使用してすべてのSIDが使用不可能になっている。すべての特権はレベル2と同じように除去されている。

【0052】

既存のトークンから制限付きトークンを作成するために、NtFilterTokenと名付けられたアプリケーション・プログラミング・インターフェース（API）が提供され、その内容は次のとおりである。

【0053】

【表3】

NTSTATUS
NtFilterToken (
IN HANDLE ExistingTokenHandle,
IN ULONG Flags,
IN PTOKEN_GROUP SideToDisable OPTIONAL,
IN PTOKEN_PRIVILEGS PrivilegeToDelete OPTIONAL,
IN PTOKEN_GROUP RestrictingSids OPTIONAL,
OUT PHANDLE NewTokenHandle
);

【0054】

NtFilterToken APIは、CreateRestrictedTokenと名付けられたWin32 APIの下でラップされ、Create

RestrictedTokenの内容は次のとおりである。

【0055】

【表4】

```

WINADVAPI
BOOL
APIENTRY
CreateRestrictedToken(
    IN HANDLE ExistingTokenHandle,
    IN DWORD Flags,
    IN DWORD DisableSidCount,
    IN PSID_AND_ATTRIBUTES SidsToDisable OPTIONAL,
    IN DWORD DeletePrivilegeCount,
    IN PLUID_AND_ATTRIBUTES PrivilegesToDelete OPTIONAL,
    IN DWORD RestrictedSidCount,
    IN PSID_AND_ATTRIBUTES SidsToRestrict OPTIONAL,
    OUT PHANDLE NewTokenHandle
);

```

【0056】

図8および図10～11に表示されたように、これらのAPI126は共同して機能し、制限付きでも制限なしでも既存のトークン100をとり、変更された（制限付き）トークン124をそこから作成する。ログオンしたユーザーのインスタンスに関する識別情報を含む制限付きトークンの構造は、ParentTokenId, RestrictedSidCount、およびRestrictedSidsの3つの新しいフィールドを含む（次の表で太字で示されている）。

【0057】

【表5】


```

Typedef struct _TOKEN {
    TOKEN_SOURCE TokenSource;           // Ro: 16-Bytes
    LUID TokenId;                       // Ro: 8-Bytes
    LUID AuthenticationId;              // Ro: 8-Bytes
    LUID ParentTokenId;               // Ro: 8-Bytes
    LARGE_INTEGER ExpirationTime;       // Ro: 8-Bytes
    LUID ModifiedId;                   // Wr: 8-Bytes

    ULONG UserAndGroupCount;            // Ro: 4-Bytes
    ULONG RestrictedSidCount;         // Ro: 4-Bytes
    ULONG PrivilegeCount;               // Ro: 4-Bytes
    ULONG VariableLength;               // Ro: 4-Bytes
    ULONG DynamicCharged;               // Ro: 4-Bytes

    ULONG DynamicAvailable;             // Wr: 4-Bytes (Mod)
    ULONG DefaultOwnerIndex;            // Wr: 4-Bytes (Mod)
    PSID_AND_ATTRIBUTES UserAndGroups;  // Wr: 4-Bytes (Mod)
    PSID_AND_ATTRIBUTES RestrictedSids; // Ro: 4-Bytes
    PSID PrimaryGroup;                 // Wr: 4-Bytes (Mod)
    PLUID_AND_ATTRIBUTES Privileges;    // Wr: 4-Bytes (Mod)
    PULONG DynamicPart;                // Wr: 4-Bytes (Mod)
    PACL DefaultDacl;                  // Wr: 4-Bytes (Mod)

    TOKEN_TYPE TokenType;               // Ro: 1-Byte

```

【0058】

【表6】

```

SECURITY_IMPERSONATION_LEVEL
    ImpersonationLevel; // Ro: 1-Byte

    UCHAR TokenFlags;           // Ro: 4-Bytes
    BOOLEAN TokenInUse;         // Wr: 1-Byte

    PSECURITY_TOKEN_PROXY_DATA ProxyData; // Ro: 4-Bytes
    PSECURITY_TOKEN_AUDIT_DATA AuditData; // Ro: 4-Bytes
    ULONG VariablePart;          // Wr: 4-Bytes (Mod)
} TOKEN, * PTOKEN;

```

【0059】

通常の（制限なしの）トークンが⁴⁰CreateToken APIを介して作成されるとき、RestrictedSidsフィールドもParentTokenIdフィールドも空であることに注意されたい。

【0060】

制限付きトークン124を作成するために、このプロセスは適切なフラグ設定および／または入力フィールドの情報を伴うCreateRestricted

Token APIを呼び出し、これはNtFilterToken APIを順番に起動する。図10のステップ1000の初めに示すように、NtFilterToken APIは、DISABLE_MAX_SIDSと名付けられたフラグが設定されているかどうかをチェックする。このフラグは、新しい、制限付きトークン124の中にあるグループに関してすべてのセキュリティIDがUSE_FOR_DENY_ONLYとマークされていなければならないことを示す。このフラグは、各々のグループを個別に識別する必要なく、トークン内のグループ（多くのグループである可能性がある）に制限を行う便利な方法を提供する。フラグが設定されている場合、ステップ1000はステップ1002に分岐し、ステップ1002では新しいトークン124内のグループ・セキュリティIDの各々について、USE_FOR_DENY_ONLYを示すビットを設定する。

【0061】

DISABLE_MAX_SIDSフラグが設定されていない場合、ステップ1000はステップ1004に分岐し、NtFilterToken APIのSidsToDisableフィールド内にセキュリティIDが個別にリストされているかどうかをテストする。図10のステップ1004で示されたように、オプションのSidsToDisable入力フィールドが存在するとき、ステップ1006では、そこにリストされ、また、親トークン100のUserAndGroupsフィールド102内にも存在する任意のセキュリティIDは、新しい制限付きトークン124のUserAndGroupsフィールド128内でUSE_FOR_DENY_ONLYとして個別にマークされる。上記のようにこのようなセキュリティIDは、アクセスを拒否するためにのみ使用でき、アクセスを許可するためには使用できず、さらに、あとから削除または使用可能にはできない。したがって、図8に示された例では、グループ₂のセキュリティIDは、NtFilterToken API126のSidsToDisable入力フィールド内にグループ₂セキュリティIDを指定することにより、制限付きトークン124内でUSE_FOR_DENY_ONLYとしてマークされる。

【0062】

フィルタ・プロセスはついで図10のステップ1010に続き、ここではDISABLE_MAX_PRIVILEGESと名付けられたフラグがテストされる。このフラグは同様に、新しい、制限付きトークン124内のすべての特権を削除すべきであることを示す、便利なショートカットとして設定できる。このように設定された場合、ステップ1010はステップ1012に分岐し、ステップ1012では新しいトークン124からすべての特権が削除される。

【0063】

フラグが設定されていない場合、ステップ1010はステップ1014に分岐し、ここではオプションのPrivilegesToDeleteフィールドが確認される。NtFilterToken API 126が呼ばれたときに存在する場合は、ステップ1016で、この入力フィールドにリストされ、また既存のトークン100の特権フィールド108にも存在する任意の特権は、新しいトークン124の特権フィールド130から個別に削除される。図8に示された例では、「特権₂」から「特権_m」として示された特権は、NtFilterToken API 126のPrivilegesToDelete入力フィールド内にこれらの特権を指定することによって、新しいトークン124の特権フィールド130から削除されている。上記のように本発明の1つの態様によれば、これは、トークン内で使用可能な特権を削減する機能を提供する。このプロセスは図11のステップ1020に続く。

【0064】

制限付きトークン124を作成するときに、ステップ1020でRestrictingSids入力フィールド内にSIDが存在していた場合、親トークンが通常のトークンか、または親トークン自体が制限付きSIDを有する制限付きトークンであるかどうかに関して決定が行われる。API、IsTokenRestrictedがステップ1022で呼び出され、親トークンのRestrictingSidsフィールドを(NtQueryInformationToken APIを介して)照会してこれがNULLでないかどうかを確認することによってこの問題を解決し、ここでNULLでなかった場合、親トークンは制

限付きトークンであり、APIはTRUE（真）を戻す。テストが満足できなかった場合、親トークンは通常のトークンでありAPIはFALSE（偽）を戻す。続くステップ1026または1028のために、トークン自体は制限付きであるが制限付きSIDを有しない親トークン（すなわち、特権が削除されているかおよび／またはUSE_FOR_DENY_ONLY SIDSである場合）は、制限付きでないとして処理される可能性があることに注意されたい。

【0065】

ステップ1024では、親トークンが制限付きである場合、ステップ1024はステップ1026に分岐し、ステップ1026では、親トークンの制限付きセキュリティIDフィールドと、APIの制限付きセキュリティID入力リストの両方にある任意のセキュリティIDは、新しいトークン124の制限付きセキュリティIDフィールド132に置かれる。制限付きセキュリティIDが両方のリストになければならないため、制限付き実行コンテキストが、制限付きセキュリティIDフィールド132にさらなるセキュリティIDを追加することを阻止し、この場合、アクセスを減らすのではなく効果的にアクセスを増やすことになる。同様に、ステップ1026で共通なセキュリティIDがなかった場合、少なくとも1つの制限付きSIDを新しいトークン内の元のトークンから取り去るなどによって、作成された任意のトークンはそのアクセスを増やすことなく制限されなければならない。その他の場合は、新しいトークン内の空の制限付きSIDフィールドはそのトークンが制限されていないことを示し、この場合、アクセスを減らすのではなく効果的にアクセスを増やすことになる。

【0066】

あるいは、ステップ1024で親トークンが通常のトークンであると判断された場合、ステップ1028で新しいトークン124のRestricting Sidsフィールド132は入力フィールド内にリストされたものに設定される。これはセキュリティIDを追加するが、次に詳細に説明されるように制限付きSIDを有するトークンが第2のアクセス・テストを受けるため、アクセスは実際には減らされることに注意されたい。

【0067】

最後に、ステップ1030も実行され、ここで新しいトークン124内のParentTokenId93は既存の（親）トークンのTokenIdに設定される。これはオペレーティング・システムに、通常は親トークン以外には許可されていないロケーションで、そのトークンの制限付きのバージョンを使用するプロセスをのちに許可するオプションを提供する。

【0068】

特に図12～14を参照して本発明の動作の説明に戻ると、図12に表示されたように、制限付きプロセス134が作成され、読み取り／書き込みアクセスでファイル・オブジェクト110を開こうと試みている。オブジェクト112のセキュリティ記述子内では、ACL120はそこにリストされた多くのセキュリティIDおよび、各IDに関して許可されたタイプのアクセスを有し、ここで「RO」は読み取りのみのアクセスが許可されていることを示し、「WR」は読み取り／書き込みアクセスを示し、「SYNC」は同期化アクセスが許可されていることを示す。他の場合は「XJones」が許可されたグループ内のメンバーシップを介してアクセスを許可されている場合でも、「XJones」は特にオブジェクト112へのアクセスを拒否されていることに注意されたい。さらに、関連付けられたこのトークン124を有するプロセス94は、このエントリーは「DENY」（すなわち、USE__FOR__DENY__ONLY）とマークされているため、トークン124内の「バスケットボール」セキュリティIDを介して任意のオブジェクトへのアクセスを許可されないことになる。

【0069】

図12に表されているように、制限付きセキュリティ・コンテキストは第1にWindows NTカーネル内で実装される。オブジェクト112へのアクセスを試みるために、プロセス134はオブジェクト・マネジャー114に、アクセスが所望されているオブジェクトを識別する情報および、所望されるアクセスのタイプを提供する（図14、ステップ1400）。オブジェクト・マネジャー114はこれに応答して、ステップ1402に表されたように、セキュリティ機構118と共同して機能し、トークン124内にリストされた（プロセス134と関連付けられている）ユーザーおよびグループ・セキュリティIDをACL1

20内のエントリーと比較し、所望のアクセスが許可されるべきか拒否されるべきかを決定する。

【0070】

ステップ1404で一般に示されているように、アクセスがリストされたユーザーまたはグループに関して許可されていない場合、セキュリティ・チェックはステップ1414でアクセスを拒否する。しかし、ステップ1404でアクセス・チェックのユーザー部分およびグループ部分の結果が許可可能なアクセスを示した場合には、セキュリティ・プロセスはステップ1406に分岐し、制限付きトークン124が任意の制限付きセキュリティIDを有しているかどうかを決定する。有していない場合、追加の制限はなく、ここでアクセス・チェックは完了し、ステップ1412において、ユーザー・アクセスおよびグループ・アクセスのみに基づいてアクセスは許可される（そのオブジェクトへのハンドルが戻される）。このようにして、通常のトークンは本質的に以前と同じようにチェックされる。しかし、ステップ1406によって決定されたように、トークンが制限付きセキュリティIDを含んでいる場合、ついでステップ1408によって、制限付きセキュリティIDをACL120内のエントリーと比較することによって、第2のアクセス・チェックが実行される。ステップ1410でこの第2のアクセス・テストがアクセスを許可した場合、そのオブジェクトへのアクセスはステップ1412で許可される。そうでない場合、アクセスはステップ1414で拒否される。

【0071】

図13で論理的に示すように、トークン124の中に制限付きセキュリティIDが存在するときはいつでも、2部分からなるテストがこのように実行される。トークン124内のセキュリティIDおよび所望のアクセス・ビット136をオブジェクト112のセキュリティ記述子に対して考慮することによって、通常のアクセス・テスト（ビットごとのAND）および制限付きセキュリティIDのアクセス・テストの両方は、プロセスがそのオブジェクトへのアクセスを許可されるようにアクセスを許可しなければならない。本発明に必要ではないが上記のように、通常のアクセス・テストが最初に行われ、アクセスが拒否された場合には

、さらなるテストは必要ではない。トークン内にACLの識別子に一致するセキュリティIDがないため、またはACLEントリーが特に、その中にあるセキュリティ識別子に基づいてトークンへのアクセスを拒否したためのどちらの理由でも、アクセスは拒否されることに注意されたい。別法としては、トークンを制限付きSIDの多数の組を有するように構成し、たとえば、組A OR (組B AND組C) がアクセスを許可するなど、これらのSIDの査定をカバーするさらに複雑なブール式を伴う場合もある。

【0072】

このように図12に示された例では、トークン124（フィールド132）内の制限付きSIDのみが「インターネット・エクスプローラ」を識別する一方、オブジェクトのACL120内には対応する制限付きSIDがないため、図12に示された例では、オブジェクト112へのアクセスはプロセス94へは許可されない。ユーザーは通常のトークンで実行するプロセスを介してオブジェクトへアクセスする権利を有していたが、プロセス94はACL内に「インターネット・エクスプローラ」SID（非DENY）を有するオブジェクトのみにアクセスできるようにするように、制限された。

【0073】

アクセスのタイプを指定する代わりに、発呼者が指定されたMAXIMUM_ALLOWEDアクセスを有する場合、これによって上記のように、アルゴリズムは最大のアクセスを決定するACL120をウォーク・スルーする。制限付きトークンで、1つでも任意のタイプのユーザー・アクセスまたはグループ・アクセスが許可された場合、ユーザーおよびグループの実行に続いて許可可能なアクセス権のタイプ（複数可）は、第2の実行に関して所望のアクセスとして指定され、第2の実行はRestrictedSidsリストをチェックする。このようにして、制限付きトークンは通常のアクセスより少ないかまたは等しいアクセスを許可されることが確認される。

【0074】

最後に、アクセス・トークンはロケーションに基づいた基準以外の基準に従ってさらに制限できることに注意されたい。実際には、制限付きトークンは、リソ

ースへアクセスしようとしているプロセス（たとえばマイクロソフト・エクセル）の識別を含む他の基準に基づいて制限付きセキュリティ・コンテキストを設定することを可能にする。さらに、種々の基準を組み合わせることでアクセス権を決定することができる。従って、たとえばユーザーがマイクロソフト・ワードではなくマイクロソフト・エクセルを介してファイルを開いている場合、ネットワーク・ファイルへのRASのアクセスが許可される場合がある。セキュリティ識別のためには事実上、ロケーションに基づいた基準と他の基準の、無限の組み合わせが可能である。

【0075】

認証

本発明の一態様によれば、クライアントがサーバに接続しているとき、サーバはクライアントを認証し、クライアントの識別およびロケーション情報に基づいてそのユーザーのためのトークンを構築する。たとえば図15および16に示されているように、よく知られたタイプの認証（すなわちNTLM）では、クライアント・ユーザ200はユーザーIDを含む認証202をサーバ204に提供し、サーバ204は次いでドメイン・サーバ206と通信してユーザーの暗号化され、格納されたパスワードに基づいてそのユーザーに関して質問を作成する。図15に表されたように、サーバ204はその質問をクライアント202に戻し、クライアントが正しく応答する場合は、そのユーザーは認証される。

【0076】

しかし本発明によれば、ユーザーに関して通常のトークンを構築するのみではなく、上に詳細に説明されたようにユーザー情報はセキュリティ・サブ・システム／プロバイダ210によってロケーション情報208と組み合わせられ、制限付きトークン212を作成する。制限付きトークン212は、任意のクライアント・プロセス216のためにサーバ204で実行されている各プロセスと関係付けられている。

【0077】

図17および18に示されたように、Kerberosプロトコルを含む他の認証プロトコルもまた本発明と共に使用できる。Kerberosプロトコルに

よれば、サーバ220への接続の認証はチケット222を介して達成される。チケット222は、最初はキー配布センタ（KDC）226として知られているネットワーク上のチケット発行機能からクライアント224によって受け取られる。チケット222はしばらくの間再使用可能であり、これによってセッションが終わった場合でも、チケット222が依然として有効な間は、クライアント130は認証プロセスを繰り返す必要はない。

【0078】

本発明によれば、上に詳細に説明されたように（クライアント224によってそこに置かれた制限を含む）チケット222内の情報は、サーバのセキュリティ・サブ・システム／プロバイダ228によってユーザーのロケーション情報230と組み合わせられ、制限付きトークン232を作成する。制限付きトークン232は任意のクライアント・プロセス236のためにサーバ220において実行されている各プロセス234と関連付けられる。

【0079】

同様に図19および20は、SSLとして知られている別の認証プロトコルを示す。SSLでは、クライアント・ユーザ240はまず公開キーに基づいた認証を使用して証明246から証明ID242を得る。サーバ248が認証機関246を信頼していると仮定して、クライアント・ユーザ240は証明ID242を使用してサーバ248へのアクセスを得る。図19に表されたように、サーバ248とクライアント240の間に往復の通信が起こり、これを介してサーバはこの証明ID242が正しいユーザーに属していることを証明できる。

【0080】

証明ID242は、ユーザーが、サーバ248が接続しているネットワークでアカウントを有していると識別するユーザー情報を含む。その情報は、そのユーザーのために維持されたユーザー情報（たとえばセキュリティID、グループID特権など）を有するデータベース250へアクセスするために使用される。次いで、上に詳細に説明されたように本発明によればデータベース250からのユーザー情報は、サーバのセキュリティ・サブ・システム／プロバイダ254によってロケーション情報252と組み合わせられて、制限付きトークン256を作

成する。制限付きトークン256は任意のクライアント・プロセス260のためにサーバ248において実行されている各プロセス258と関連付けられる。

【0081】

これらの認証プロトコルおよび別の認証プロトコルを介して得られたユーザー情報はロケーション情報と組み合わせられて、ユーザーのリソースへのアクセスを制限することが理解されたであろう。さらに、認証のタイプ自体をユーザーのロケーションに依存させることもできる。たとえば、セキュリティを増加するためにリモート接続がKerberosまたはSSL認証を必要とし、一方、ローカル接続を介して接続しているユーザーを認証するには質疑応答認証で十分である場合もある。サーバがロケーション情報へのアクセスを有するため、サーバは特定のロケーションについて必要とされる認証のタイプを決定できる。同様に、認証のタイプはアクセス権を識別するために使用することもできる。たとえば、SSLユーザーのアクセス権は1つの方法で制限し、Kerberosユーザーは別の方法で、NTLMユーザーはさらに別の方法で制限することもできる。上記の方法では、制限付きトークンはユーザーの仮想的なロケーションおよび／または認証タイプに基づいて制限付きセキュリティ・コンテキストを実装する便利な機構を提供するが、他の実施形態機構も可能である。

【0082】

本発明は種々の変形および代替の構成を可能にするが、そのうち所定の図示された実施形態が図に示され、上記に詳細に説明された。しかし、本発明を開示された具体的な形に制限する意図はなく、逆に、本発明の精神と範囲に含まれるすべての変形例、代替の構成、等価物をカバーすることが目的であることを理解されたい。

【図面の簡単な説明】

【図1】

本発明が組み入れられるコンピュータ・システムを表す構成図である。

【図2】

ユーザーがネットワークに接続する可能性のある仮想的なロケーションを一般に表す構成図である。

【図3】

本発明の一態様による、ユーザーのロケーションを決定し、そのロケーションに基づいてユーザーのアクセス・レベルを決定するために取られる一般的なステップを表す流れ図である。

【図4】

本発明の一態様による、ロケーション情報に基づいてユーザー・アクセスを確立するための種々の構成要素を一般に表す構成図である。

【図5】

本発明の一態様による、ロケーション情報に基づいてユーザーの信頼のレベルを決定するためにとられる一般的なステップを表す流れ図である。

【図6】

本発明の一態様による、ロケーション情報に基づいてユーザーの信頼のレベルを決定するためにとられる一般的なステップを表す流れ図である。

【図7】

本発明の一態様による、ユーザーのアクセス権を決定する機構を一般に表す構成図である。

【図8】

本発明の一態様による、既存のトークンから制限付きトークンを作成することを一般に表す構成図である。

【図9】

プロセスがリソースにアクセスできるかどうかを決定するための種々の構成要素を一般に表す構成図である。

【図10】

本発明の一態様による、既存のトークンから制限付きトークンを作成するためにとられる一般的なステップを表す流れ図である。

【図11】

本発明の一態様による、既存のトークンから制限付きトークンを作成するためにとられる一般的なステップを表す流れ図である。

【図12】

本発明の一態様による、リソースへのアクセスを試み、関連付けられた制限付きトークンを有するプロセスを一般に表す構成図である。

【図13】

本発明の一態様による、関連付けられた制限付きトークンを有するプロセスのオブジェクトへのアクセスを決定するための論理を一般に表す構成図である。

【図14】

本発明の一態様による、リソースへのプロセスアクセスを許可するかどうかを決定するときにとられる一般的なステップを表す流れ図である。

【図15】

質疑応答認証プロトコル内でクライアントとサーバの間の通信を表す図である。

【図16】

本発明の一態様による、認証証明およびロケーション識別に基づいて制限付きトークンを作成することを表す構成図である。

【図17】

Kerberos 認証プロトコルに従って、サーバにおいてクライアントを認証するための通信を表す図である。

【図18】

本発明の一態様による、認証チケットおよびロケーション識別に基づいて制限付きトークンを作成することを表す構成図である。

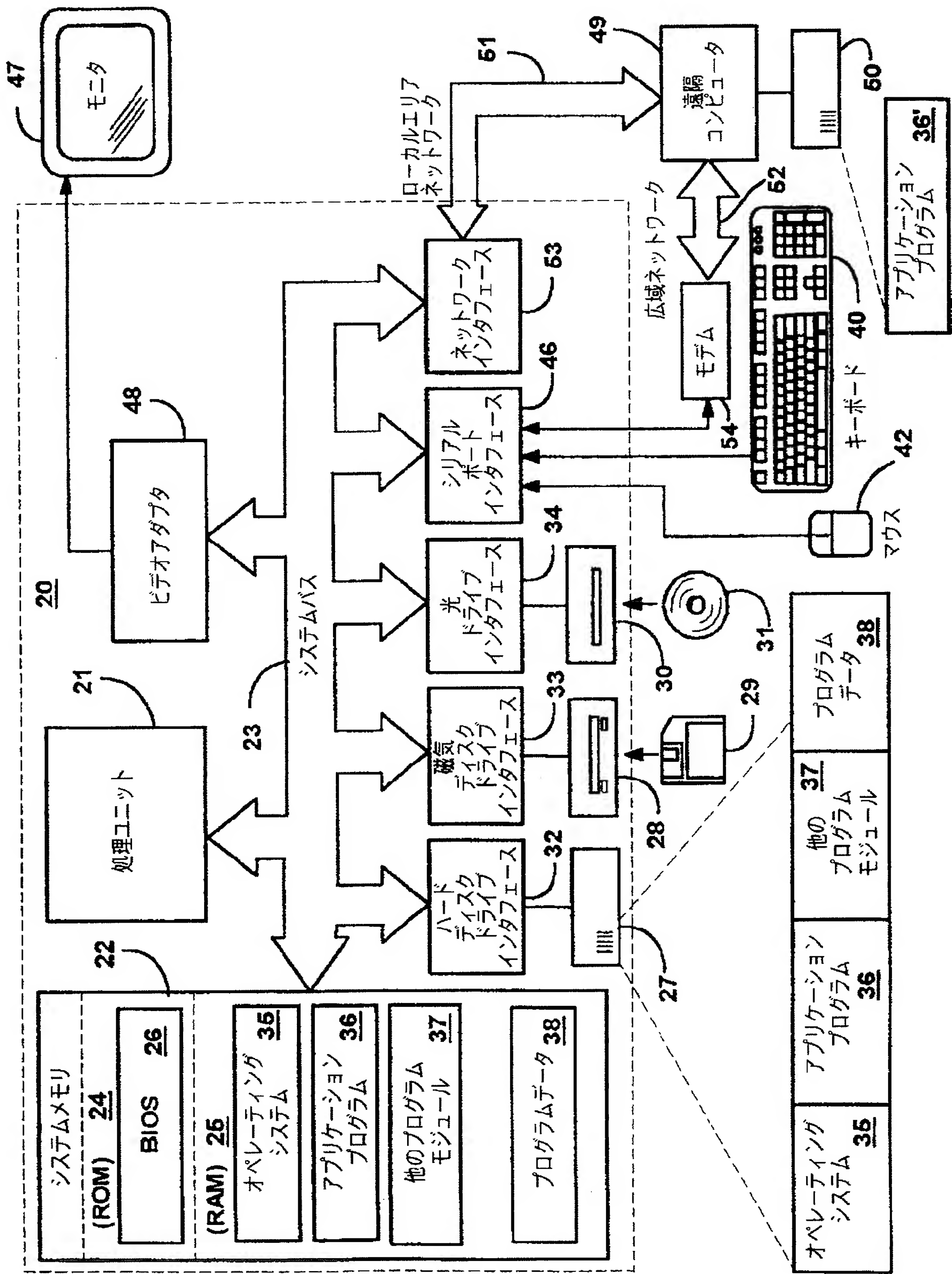
【図19】

SSLプロトコルに従って、サーバにおいてクライアントを認証するための通信を表す図である。

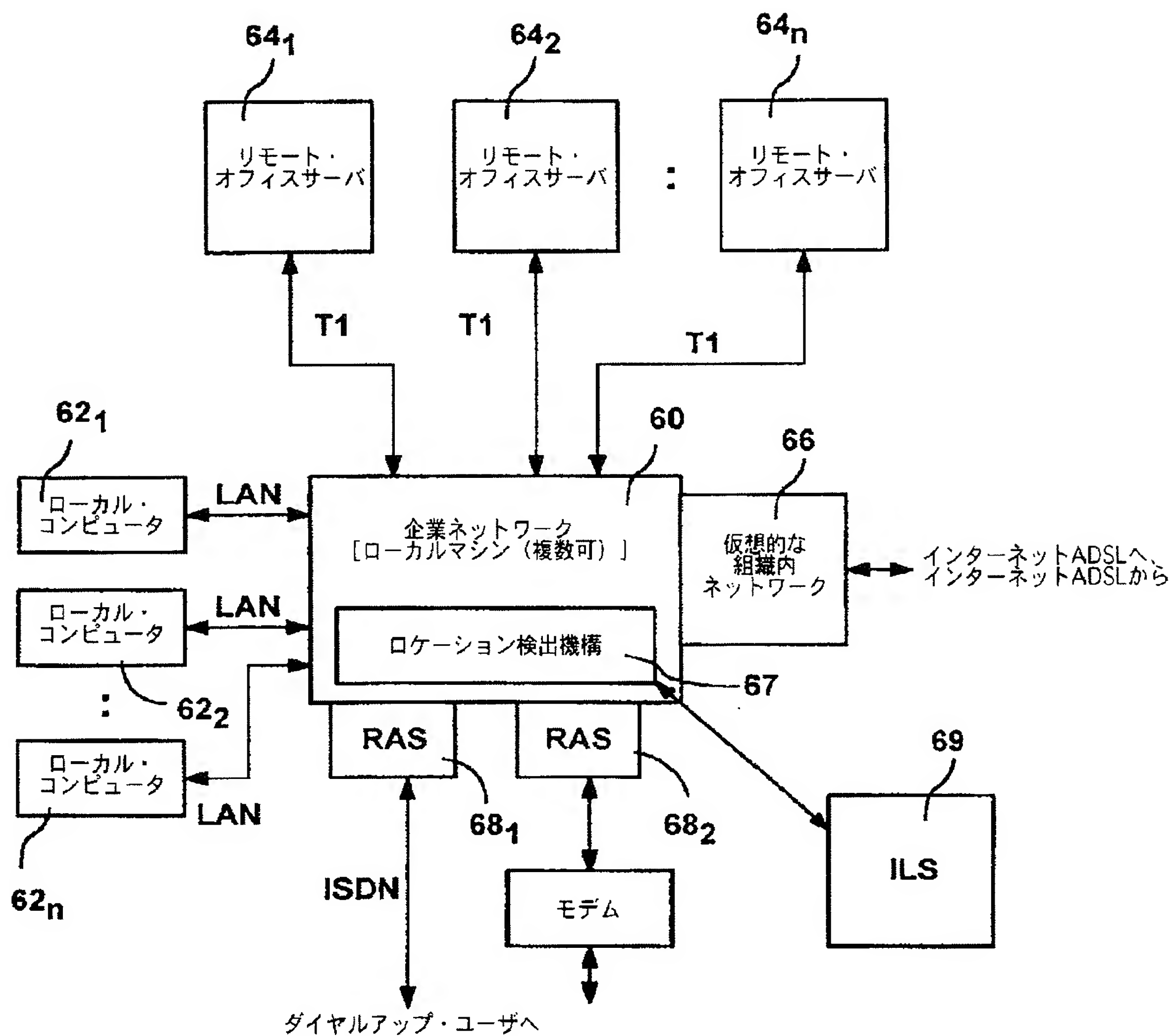
【図20】

本発明の一態様による、認証証明およびロケーション識別に基づいて制限付きトークンを作成することを表す構成図である。

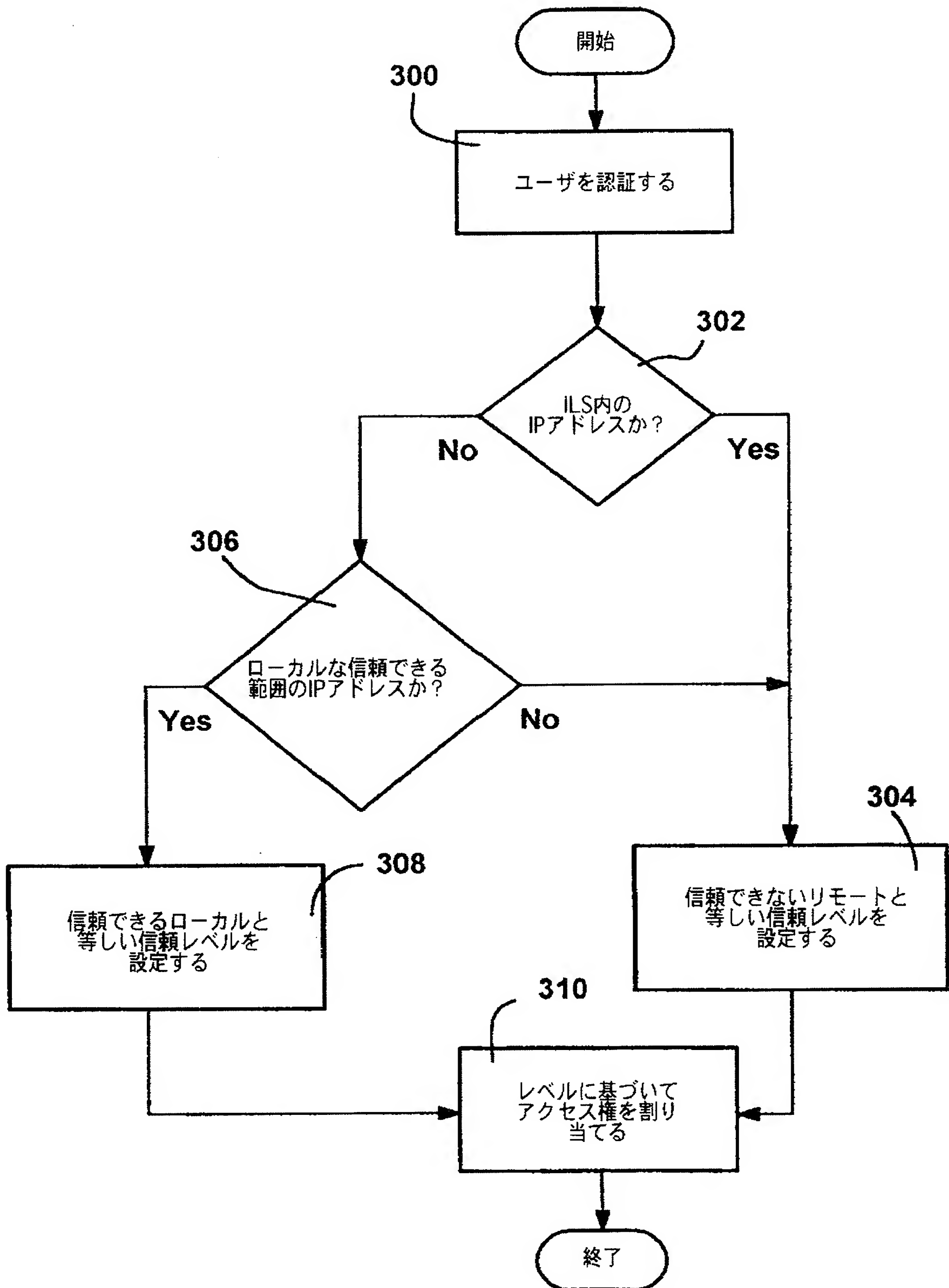
【図1】



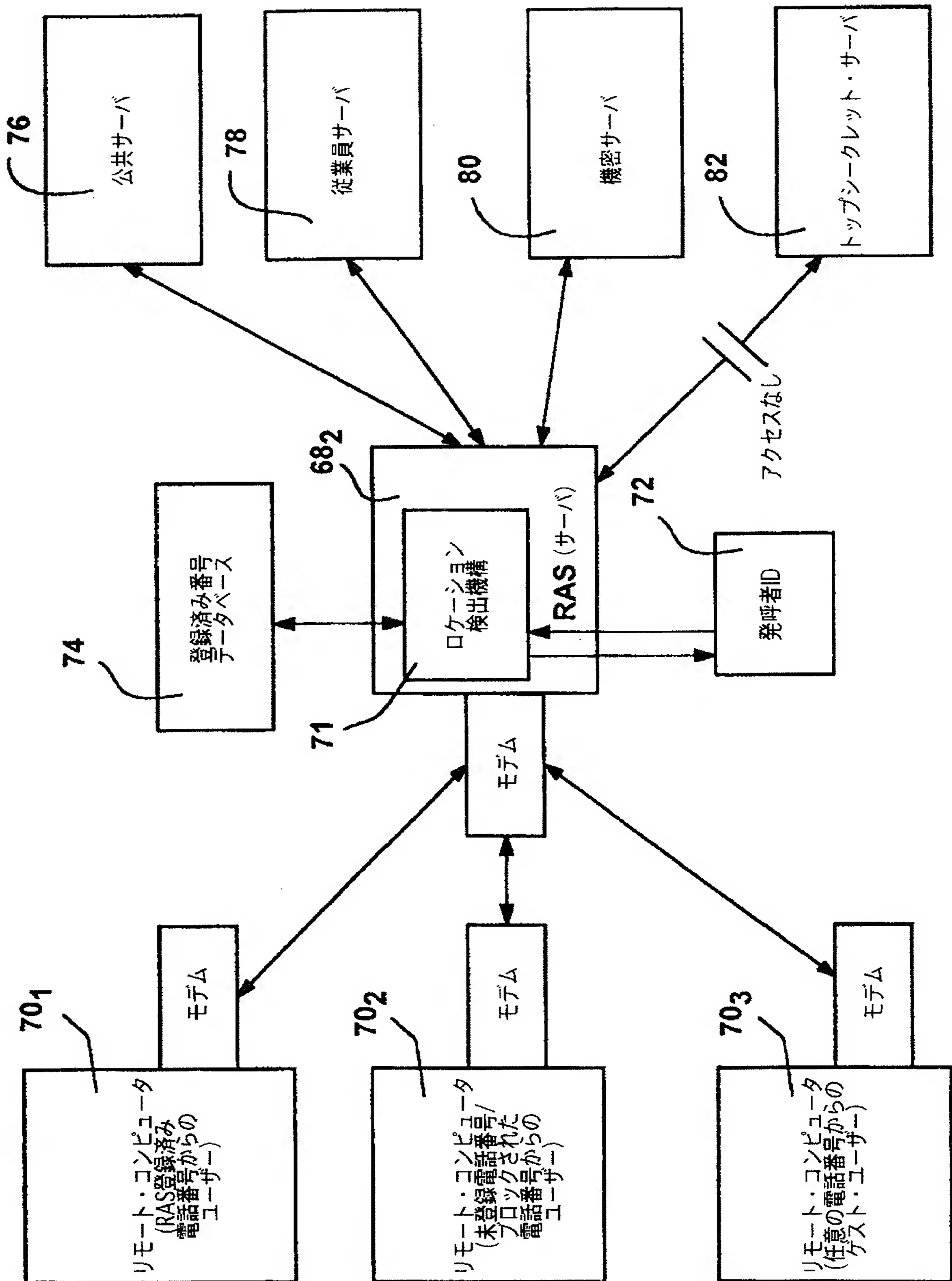
【図2】



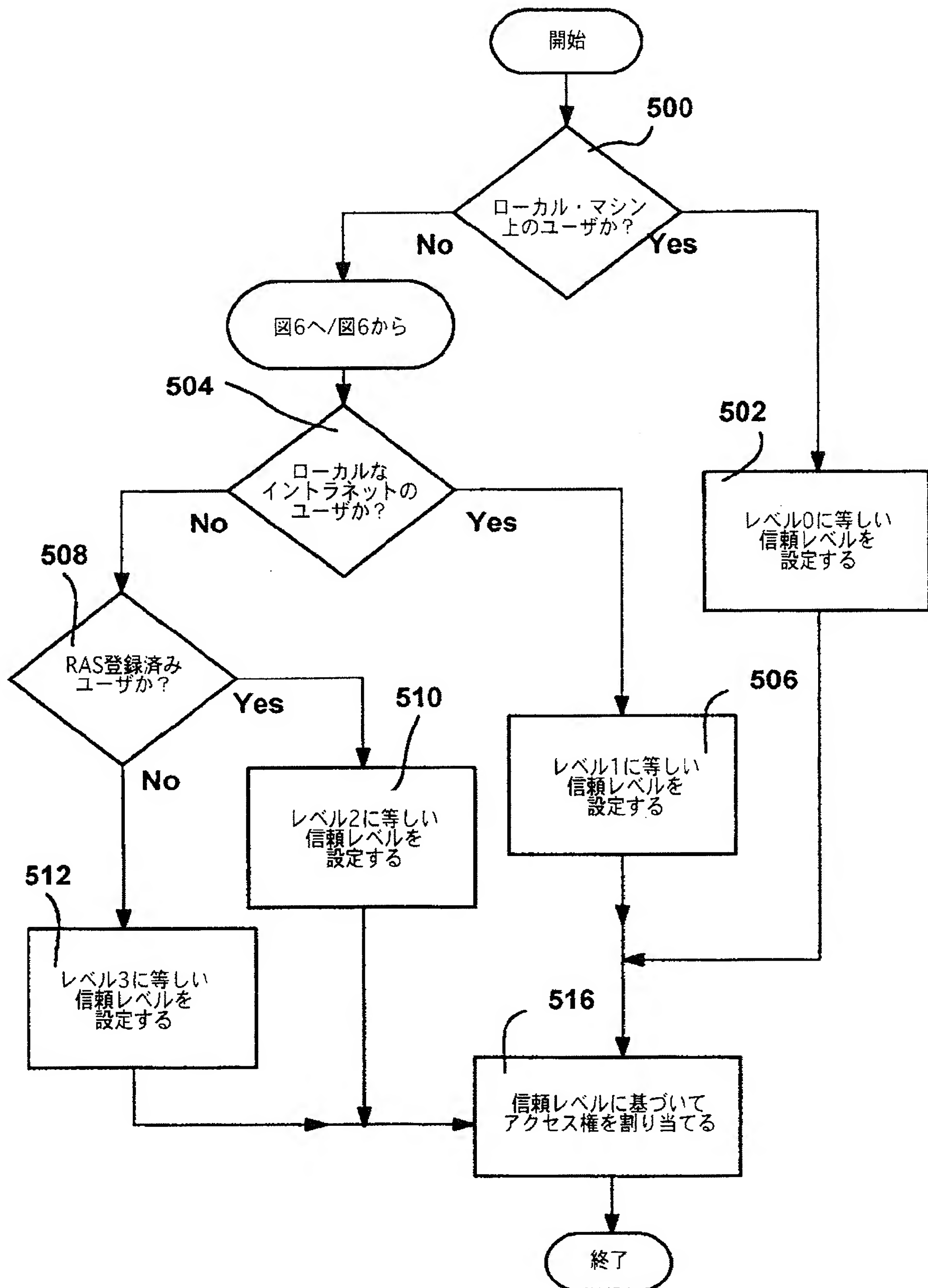
【図3】



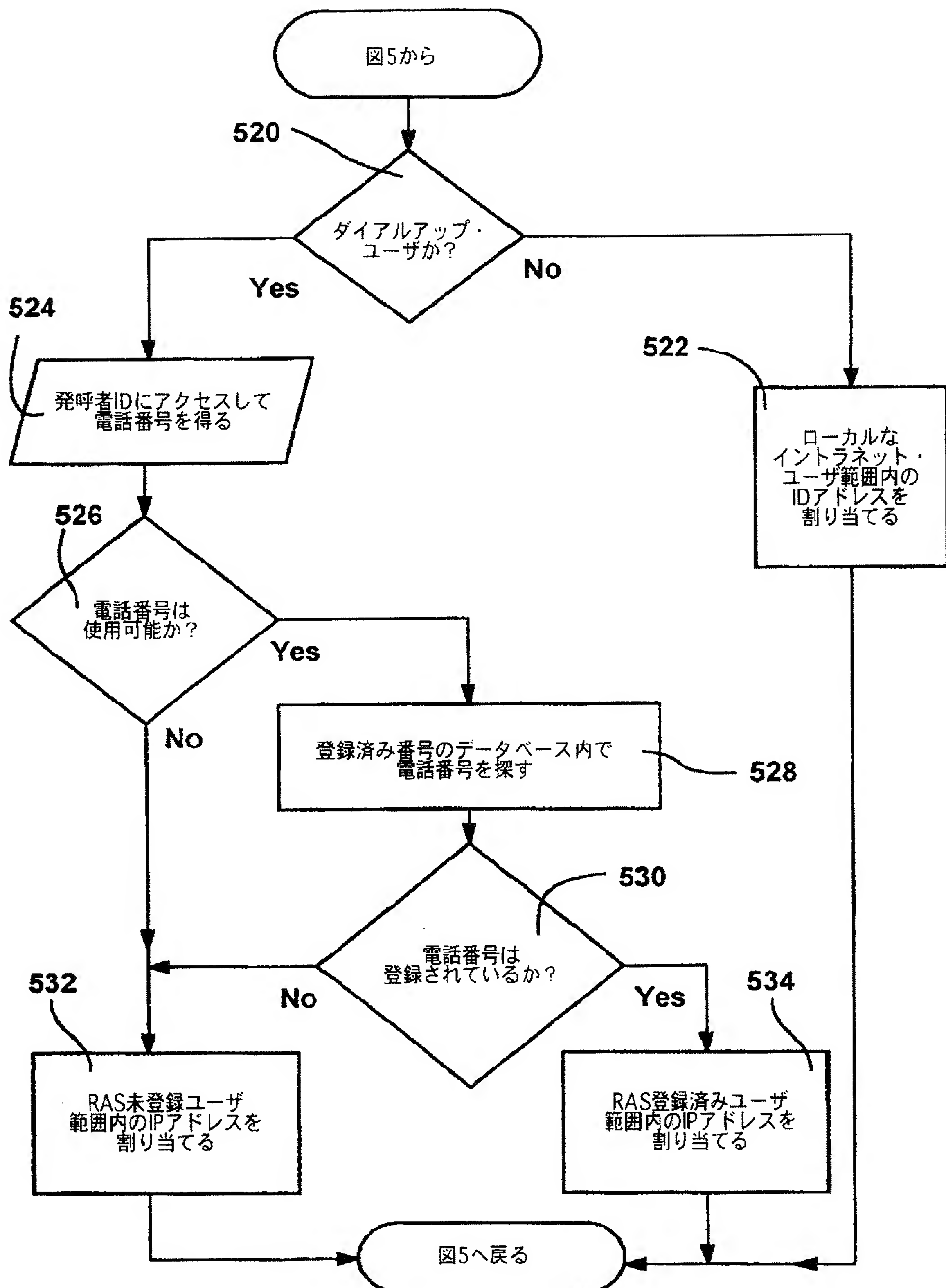
【図4】



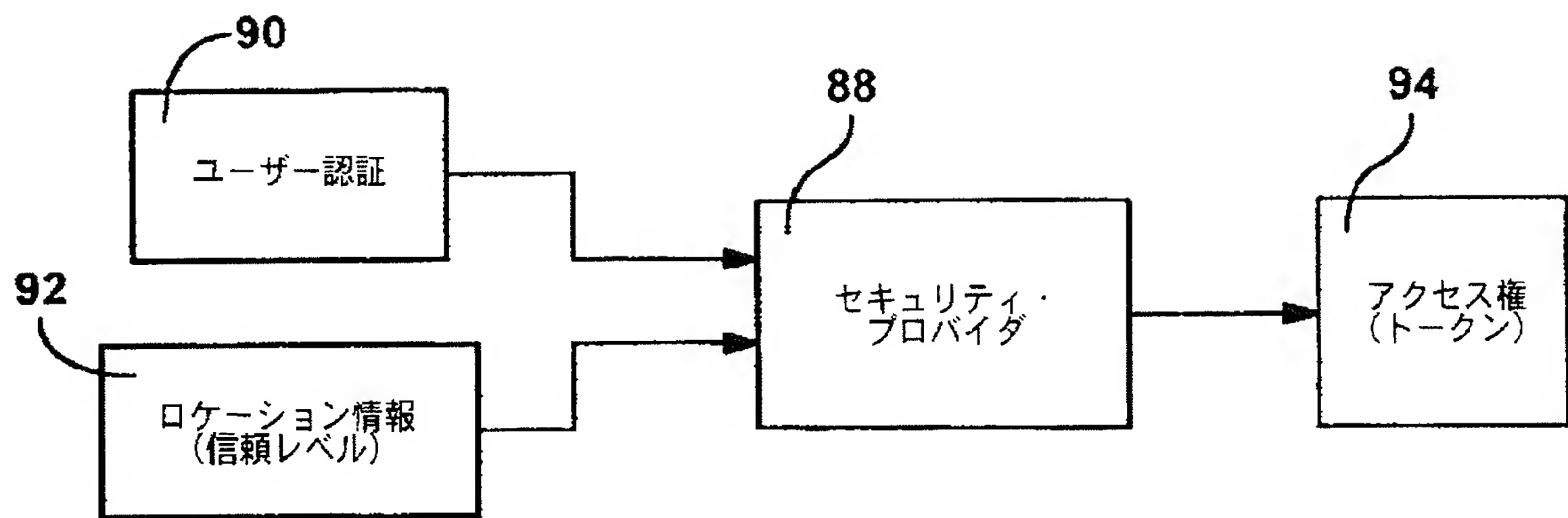
【図5】



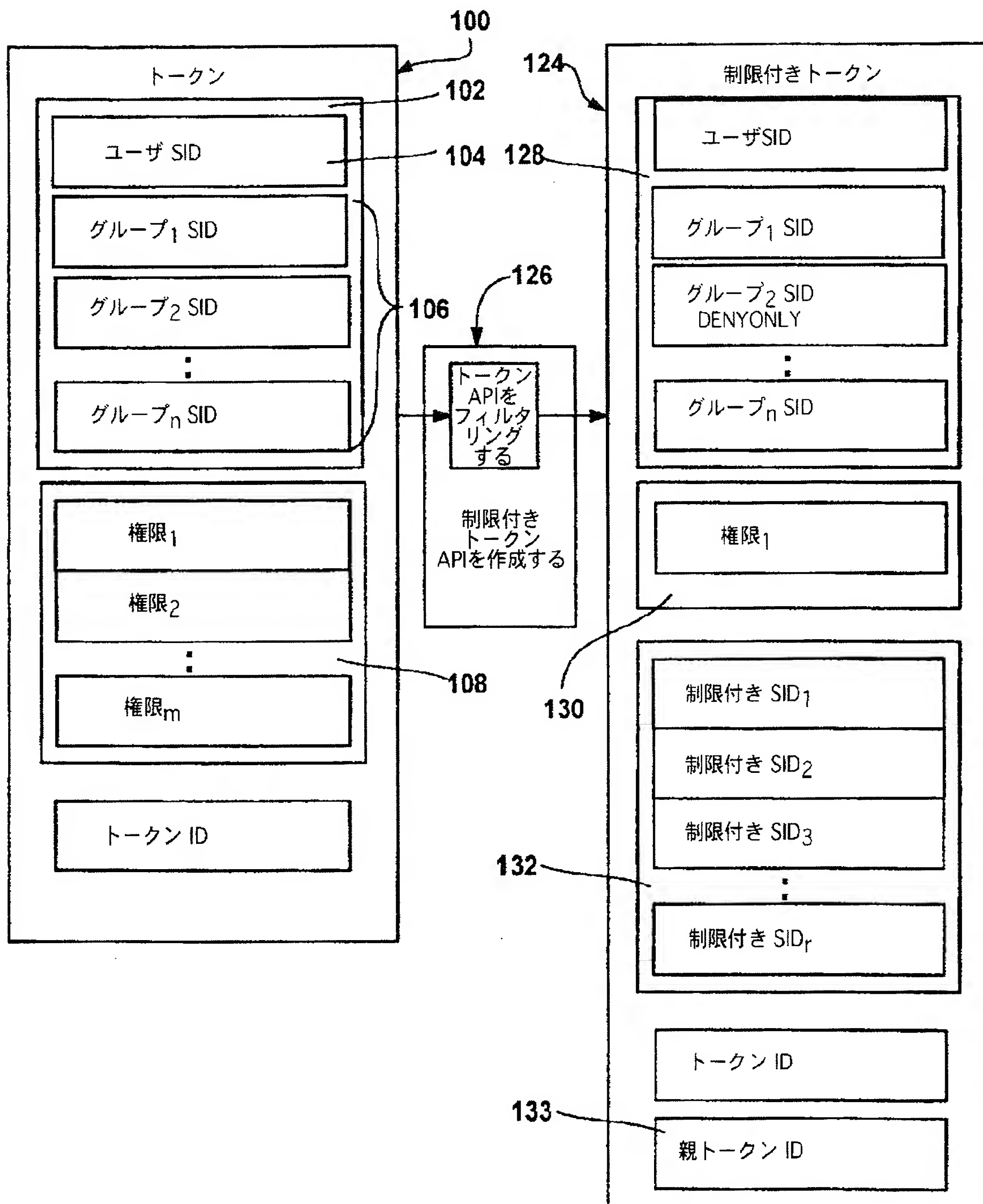
【図6】



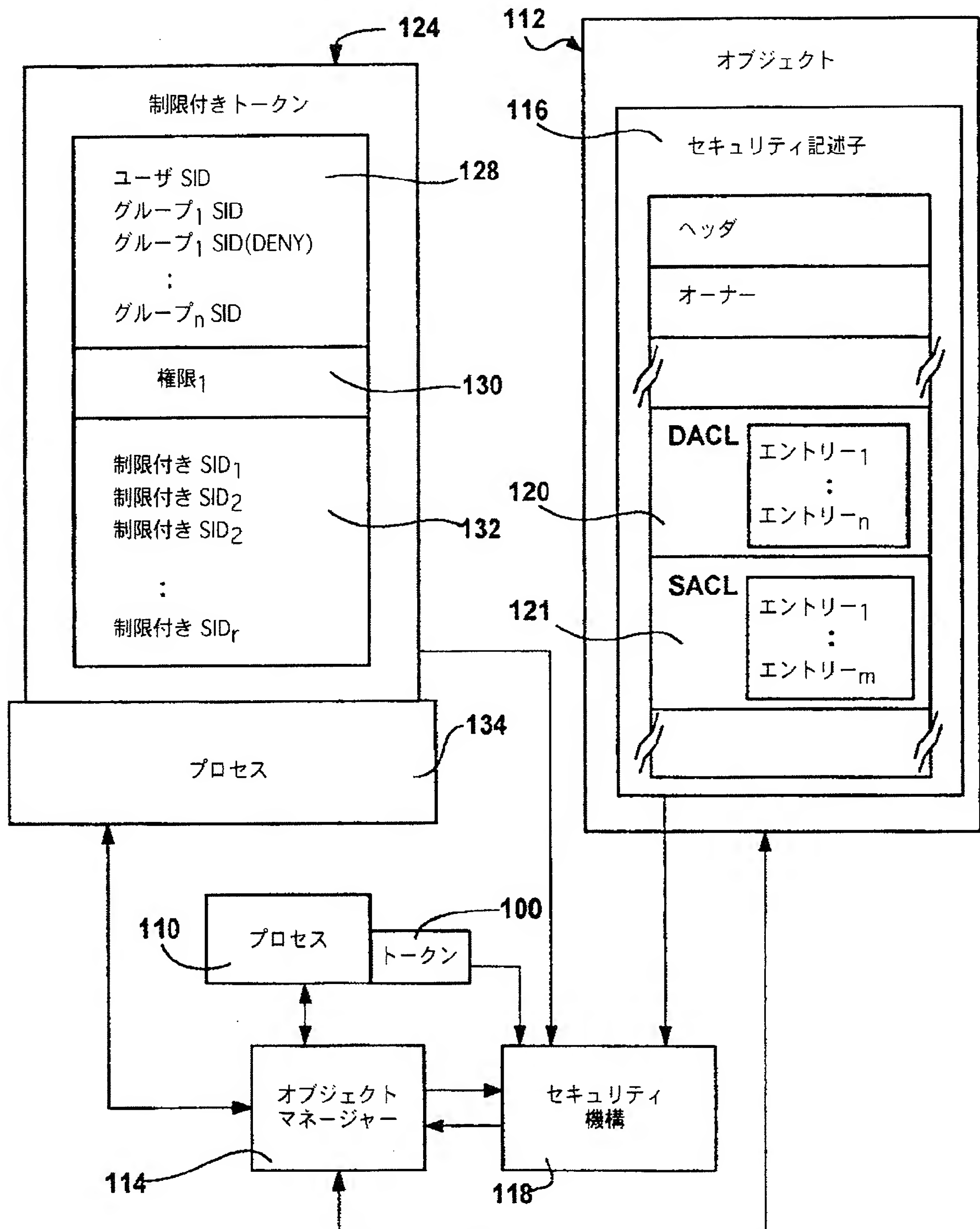
【図7】



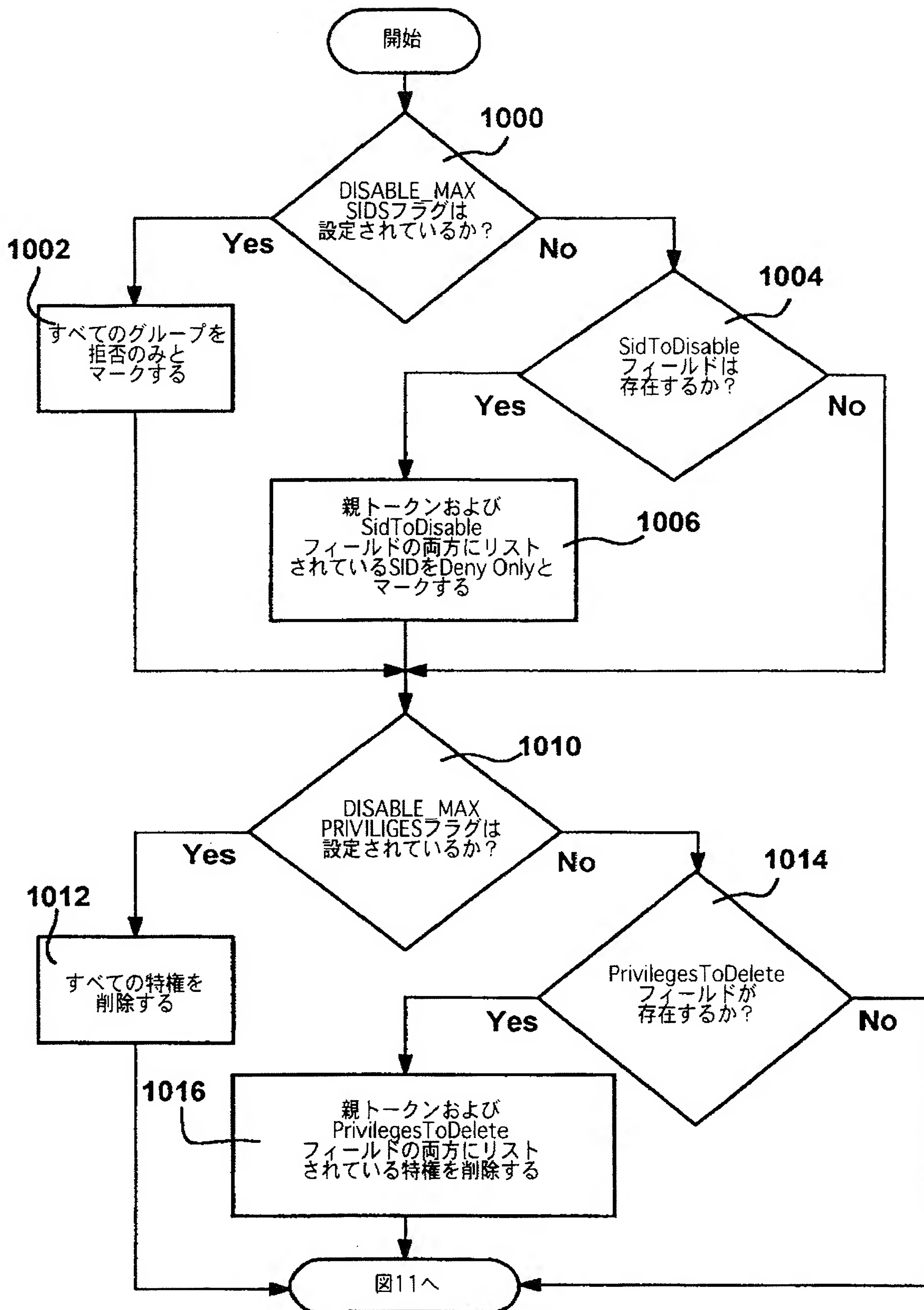
【図 8】



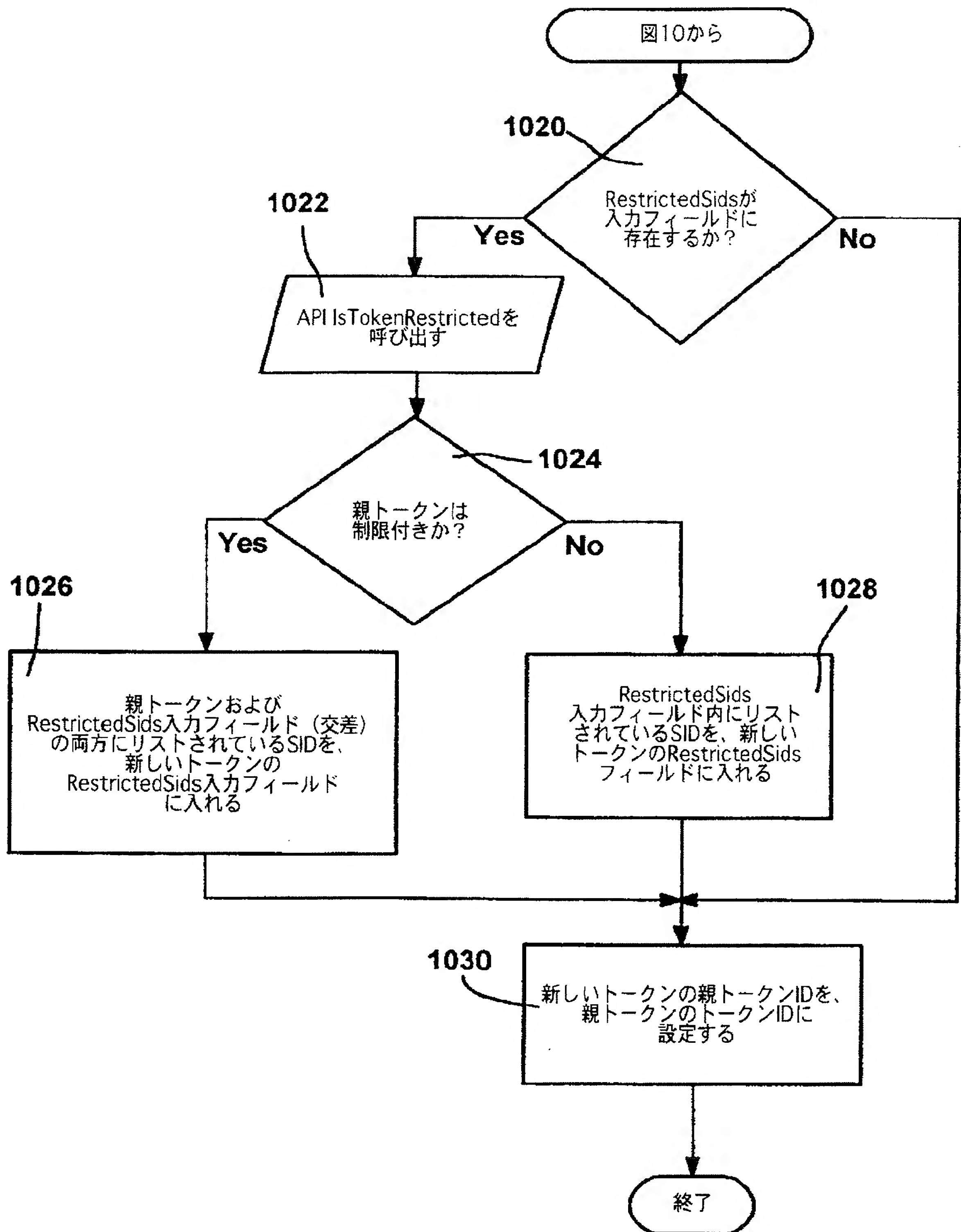
【図 9】



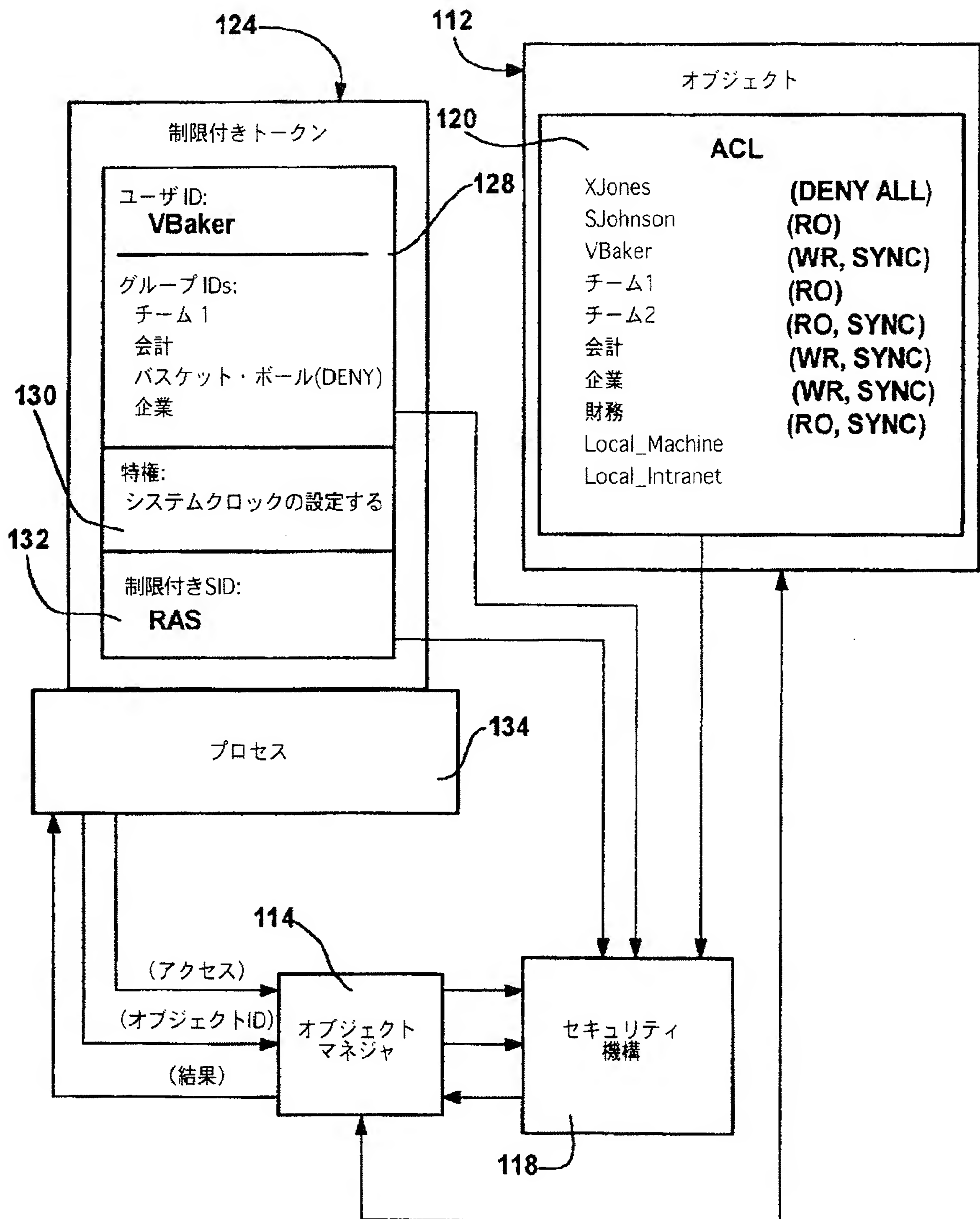
【図10】



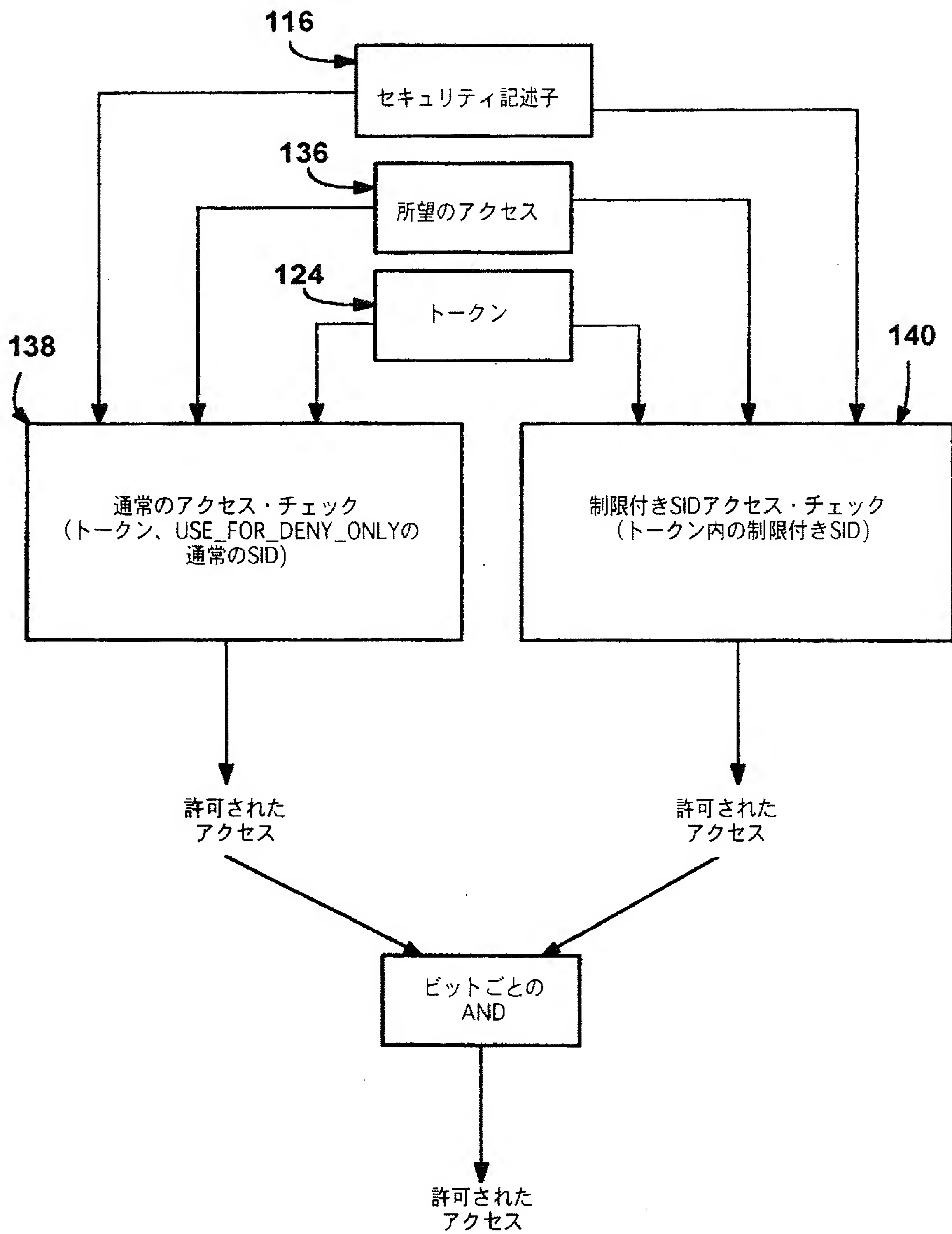
【図11】



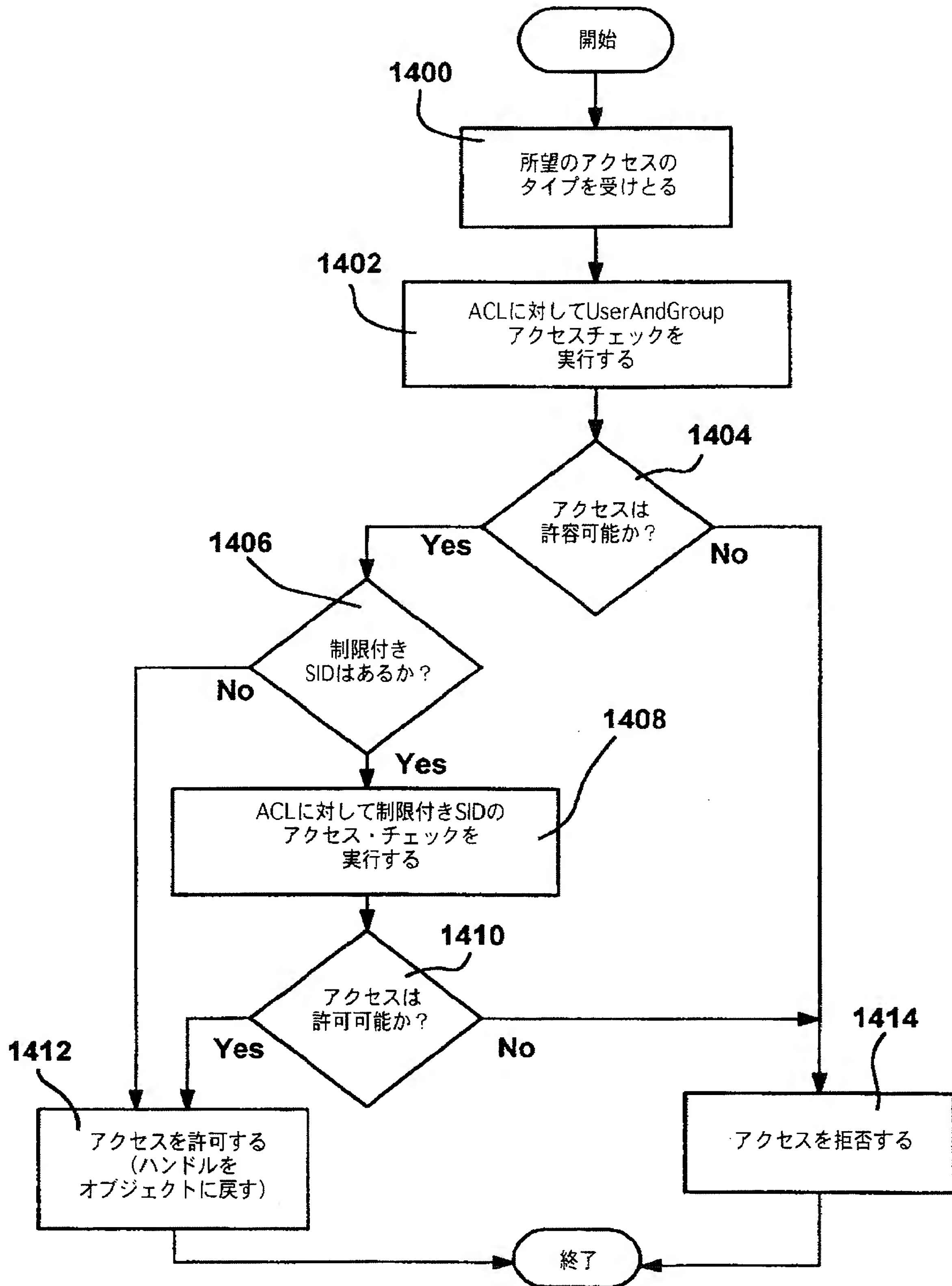
【図12】



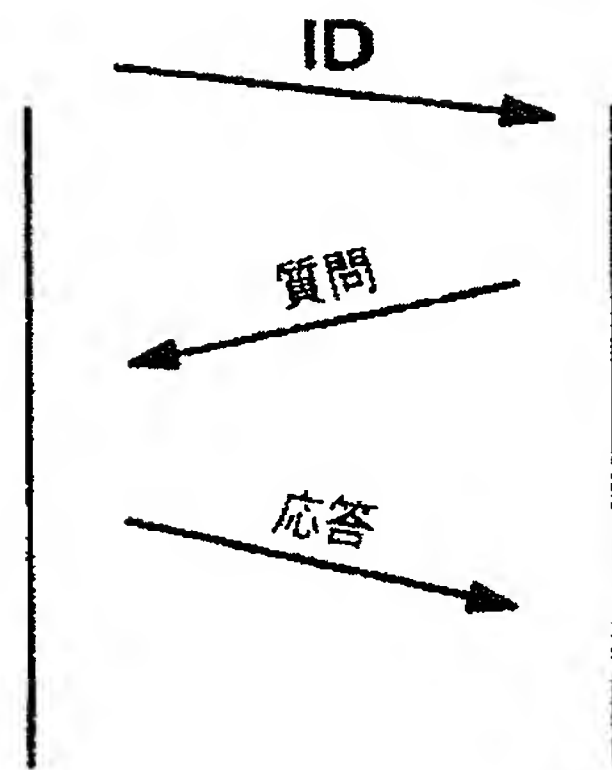
【図13】



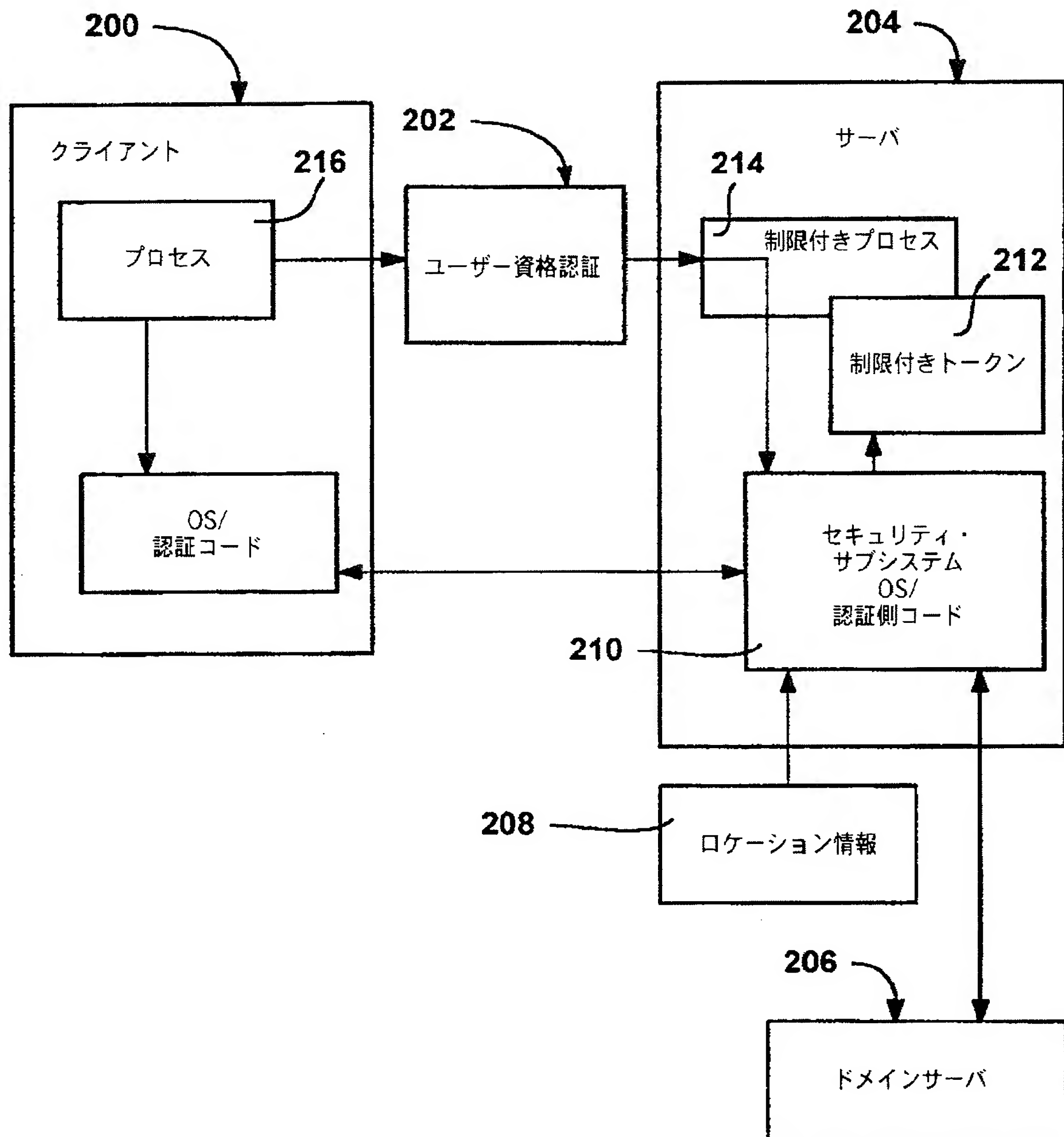
【図14】



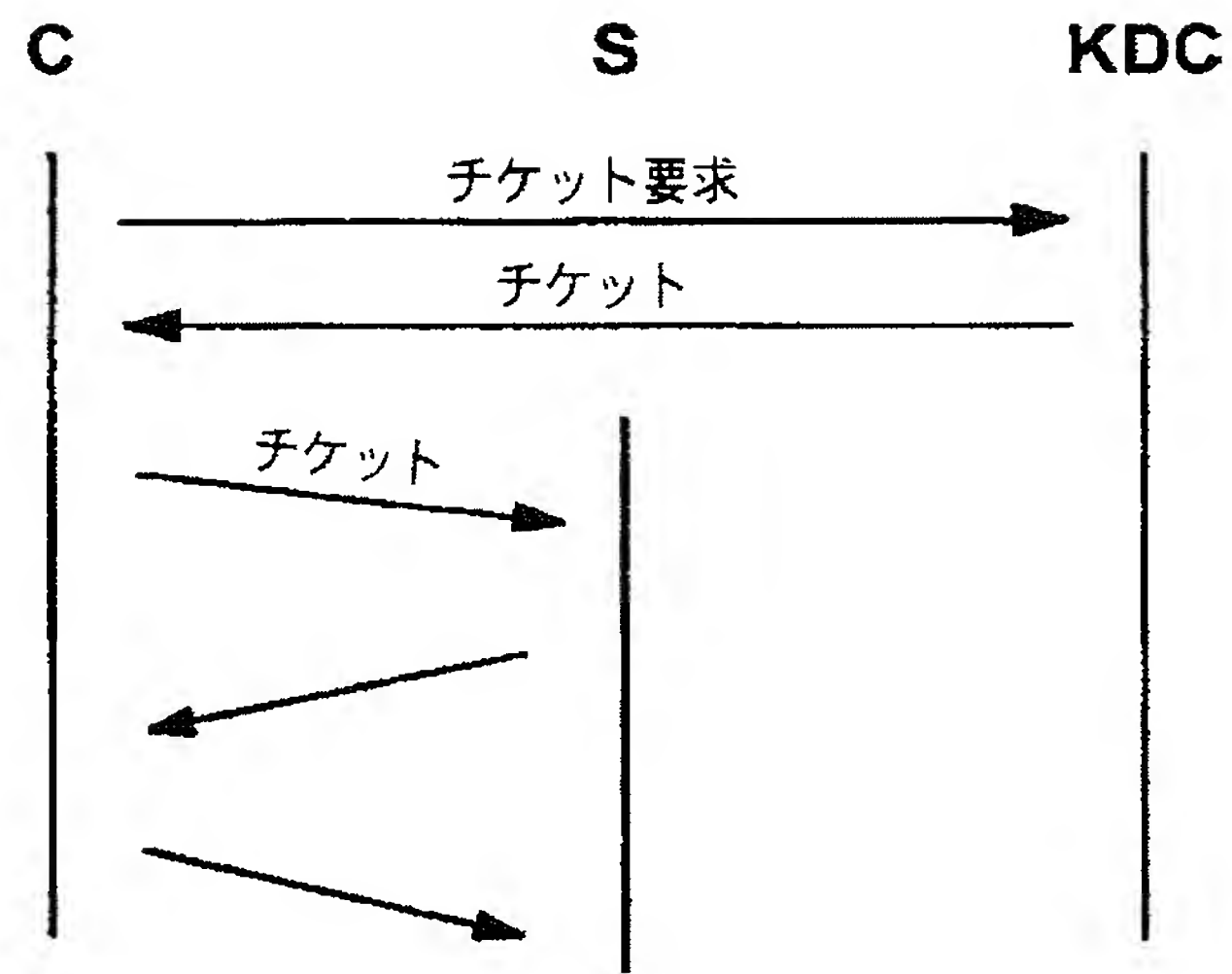
【図 1 5】



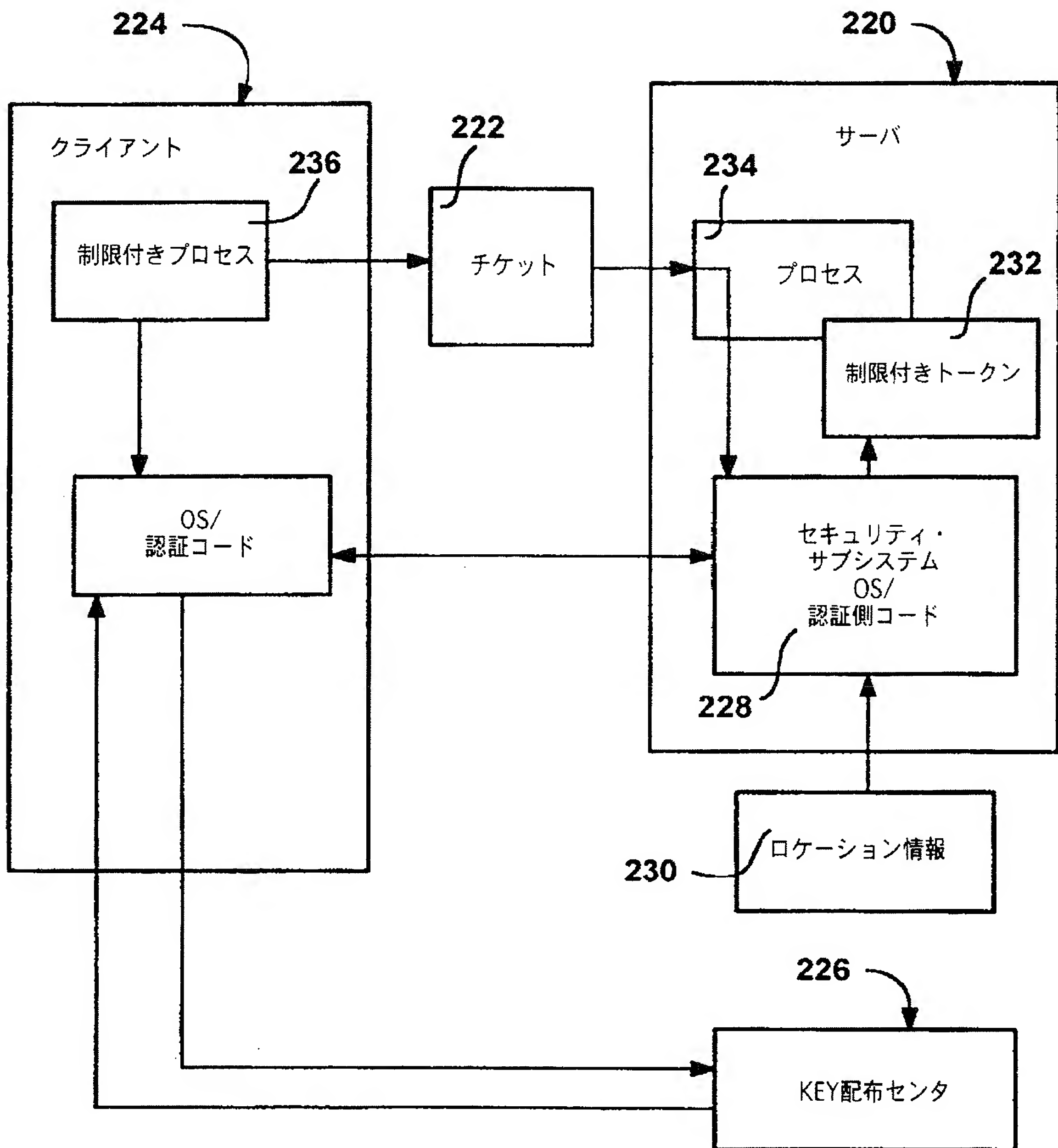
【図16】



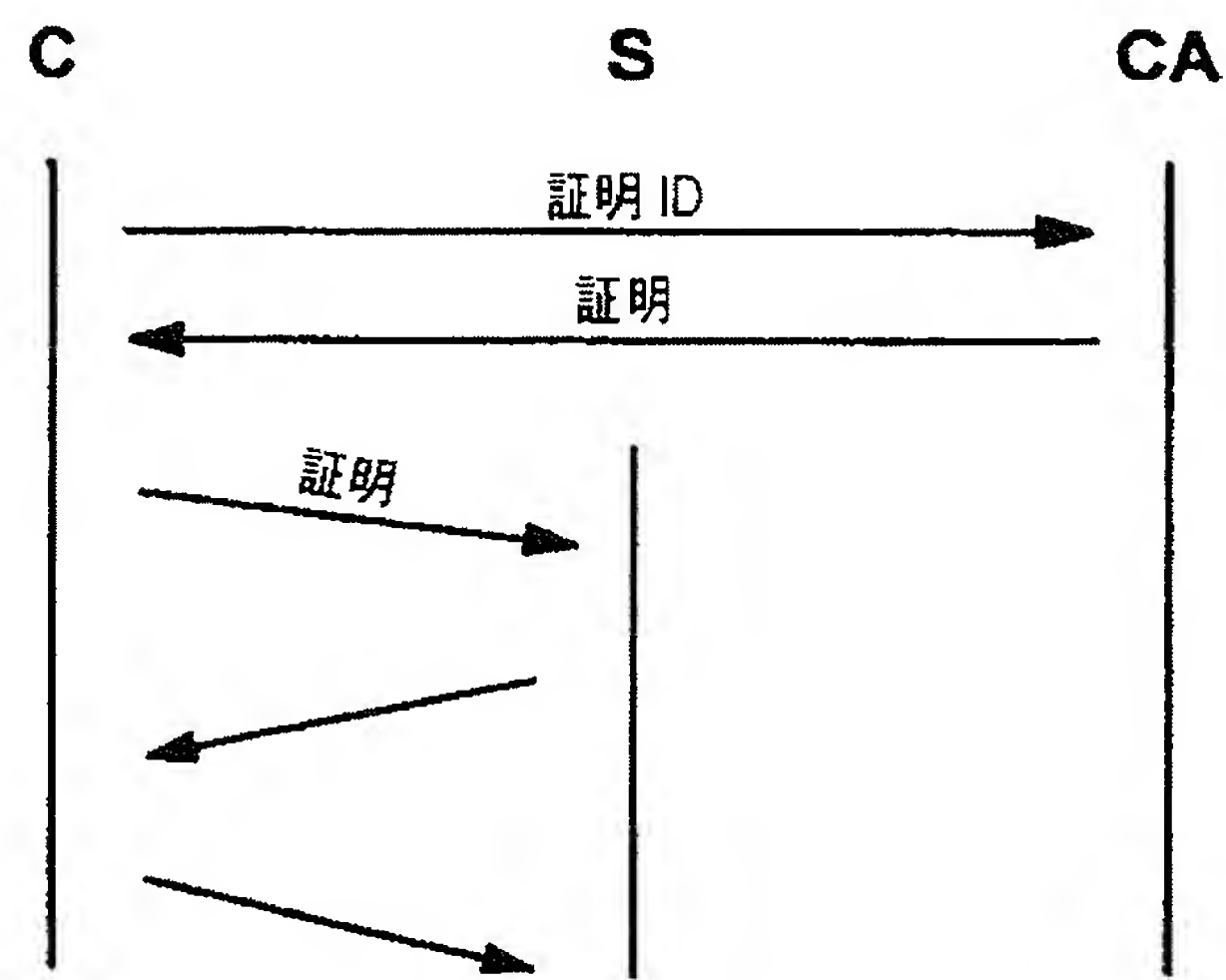
【図17】



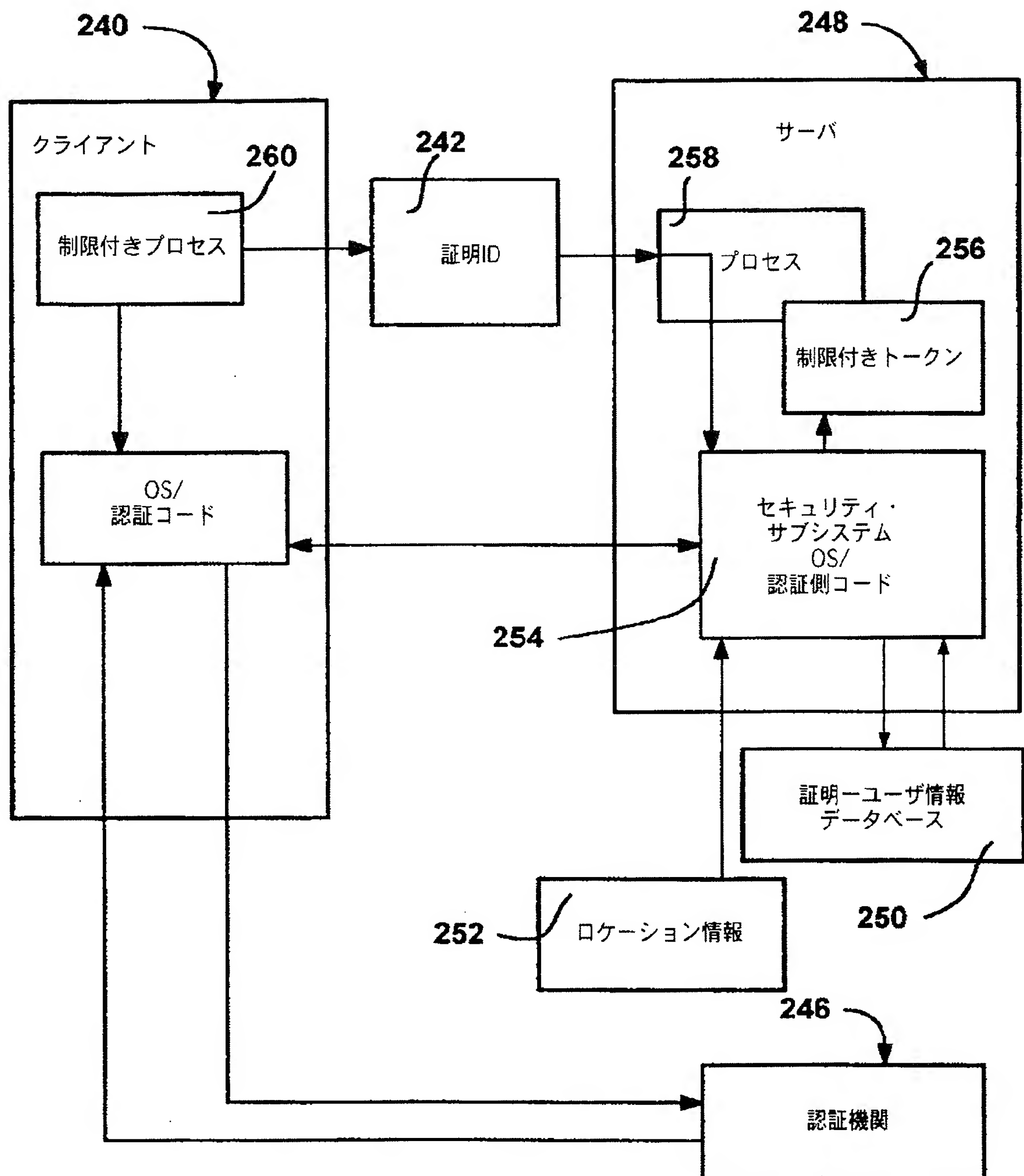
【図18】



【図 1 9】



【図20】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No.

PCT/US 99/12913

A. CLASSIFICATION OF SUBJECT MATTER

IPC 6 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 96 05549 A (SHIVA CORPORATION) 22 February 1996 (1996-02-22) page 8, line 9 -page 9, line 12 ----	1,21,34
A	EP 0 465 016 A (DIGITAL EQUIPMENT CORPORATION) 8 January 1992 (1992-01-08) column 4, line 26 -column 5, line 28 -----	1,21,34

☐ Further documents are listed in the continuation of box C.☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

11 October 1999

Date of mailing of the international search report

18/10/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Ströbeck, A

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/US 99/12913

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9605549 A	22-02-1996	AU 3099295 A	07-03-1996
		CA 2197219 A	22-02-1996
		DE 69510551 D	05-08-1999
		EP 0775341 A	28-05-1997
EP 0465016 A	08-01-1992	US 5204961 A	20-04-1993
		CA 2044003 A,C	26-12-1991
		DE 69130657 D	04-02-1999
		DE 69130657 T	22-07-1999
		JP 1996980 C	08-12-1995
		JP 6095991 A	08-04-1994
		JP 7031648 B	10-04-1995

フロントページの続き

(72) 発明者 スージ イー. ストロム
アメリカ合衆国 98053 ワシントン州
レッドモンド ノースイースト 239 ア
ベニュー 413

(72) 発明者 プラエリット ガーグ
アメリカ合衆国 98034 ワシントン州
カークランド ノースイースト 104 ア
ベニュー 12648

(72) 発明者 バーラト シャー
アメリカ合衆国 98059 ワシントン州
ニューキャッスル サウスイースト 136
アベニュー 8223

Fターム(参考) 5B085 AE06 BC02